National Nuclear Security Administration

Policy Letter: NAP-14.1
Date: September 12, 2003

NOTE: See Paragraph 8 of this Policy Letter for a listing of associated DOE Directives implemented by the NNSA PSCP.

TITLE: NNSA Cyber Security Program

1. INTRODUCTION. All information collected, created, processed, transmitted, stored, or disseminated by, or on behalf of, the National Nuclear Security Administration (NNSA) on automated information systems requires some level of protection. The loss or compromise of information entrusted to NNSA or its contractors may affect the Nation's economic competitive position, the environment, the national security, NNSA missions, or the citizens of the United States. The risk management approach defined in the NNSA cyber security program provides for the graded, cost-effective protection of automated information systems containing unclassified or classified information.

   The NNSA Program Secretarial Office Cyber Security Program (PCSP) systematically integrates cyber security into management and work practices at all levels in the NNSA so that missions are accomplished while appropriately protecting all information on information systems; establishes requirements and responsibilities for protecting information on information systems for the purpose of maintaining national security and ensuring the continuity of NNSA operations; and ensures NNSA cyber security is consistent with, and achieves the objectives of Executive Orders, National Security Directives, Department of Energy (DOE) Orders and Manuals, and Federal regulations.

   - The PCSP is implemented through a Cyber Security Program Plan (CSPP) for each NNSA element.
   - Risk management in the PCSP is a process that considers the prevailing NNSA threat analysis, the attributes of the information being protected, the effect of countermeasures in place and planned, and the remaining vulnerability of the processing environment (residual risk).
   - The PCSP establishes minimum protection requirements based on the consequence of loss of confidentiality, integrity, and availability of all information.
   - Protection requirements for all information systems are documented in Security Plans.
   - The PCSP is consistent with other NNSA directives and DOE Orders and Manuals that provide specific security requirements for communications

systems, transmission systems, classified matter through administrative procedures, access authorizations, and physical security requirements.

2. OBJECTIVES.

   a. To implement DOE O 205.1, "*Departmental Cyber Security Management Program*," in the NNSA and all organizations under its cognizance.

   b. To establish an NNSA PCSP that systematically integrates cyber security into management and work practices at all levels in the NNSA so that missions are accomplished while appropriately protecting all information on information systems.

   c. To establish requirements and assign responsibilities within the NNSA PCSP for protecting information on information systems.

   d. To ensure the NNSA PCSP is consistent with, and achieves the objectives of Executive Orders, National Security Directives, DOE Orders and Manuals, and Federal regulations.

   e. To establish a NNSA cyber security process that addresses program requirements, defines protection measures, provides cyber security planning, and implements the NNSA PCSP.

   f. Implement requirements in Public Law (PUB. L.) 100-235 (1987) and the Office of Management and Budget (OMB) Circular A-130 in the NNSA and all organizations under its cognizance.

   g. Implement requirements in NSTISSP No. 6, *National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems.* This policy requires C&A of national security systems.

   h. Implement requirements in NSTISSI No. 1000 *National Information Assurance Certification and Accreditation Process (NIACAP).*

   i. Establish requirements and prescribe a process for C&A of information systems in the NNSA.

   j. Stress the importance of a life-cycle management approach to the C&A and re-accreditation of NNSA information technology.

3. CANCELLATIONS. None.

4. APPLICABILITY. This NNSA Policy (NAP) applies to all entities, Federal or contractor, that collect, create, process, transmit, store, and disseminate information for the NNSA.

a. NNSA Elements. NNSA Headquarters Organizations, Service Center, Site Offices, NNSA contractors, and subcontractors are, hereafter, referred to as NNSA elements.

b. Information System. This NAP applies to any information system that collects, creates, processes, transmits, stores, and disseminates unclassified or classified NNSA information. This NAP applies to any information system life cycle, including the development of new information systems, the incorporation of information systems into an infrastructure, the incorporation of information systems outside the infrastructure, the development of prototype information systems, the reconfiguration or upgrade of existing systems, and legacy systems. In this document, the term(s) "information system," or "system" are used to mean any information system or network that is used to collect, create, process, transmit, store, or disseminate data owned by, for, or on behalf of NNSA or DOE.

c. Exclusion.

(1) The Deputy Administrator for Naval Reactors shall, in accordance with the responsibilities and authorities assigned by Executive Order 12344 (set forth in Public Law 106-65 of October 5, 1999 [50 U.S.C. 2406]) and to ensure consistency throughout the joint Navy and DOE Organization of the Naval Reactors Propulsion Program, implement and oversee all requirements and practices pertaining to this Order for activities under the Deputy Administrators cognizance.

(2) The NNSA PCSP does not apply to Sensitive Compartmented Information (SCI) information systems located in NNSA sites. SCI information systems must comply with Director, Central Intelligence Directives (DCID) security policies. Operation of SCI information systems is approved by the DOE Office of Intelligence.

d. Implementation. A plan for the implementation of this NAP must be completed within 60 days after issuance of this NAP.

(1) Existing Accredited Information Systems. All currently valid information system accreditations may continue in effect until the accreditation expires or re-accreditation is necessary. Re-accreditation of these systems must conform to the NNSA PCSP.

(2) Information Systems In Progress. Information systems that have begun the C&A process before release of this NAP may be accredited under the previous requirements. These systems will remain accredited until re-accreditation is required, either because the systems have passed the 3-year accreditation expiration date or because of significant changes in the security requirements of the information system. Re-accreditation must conform to the NNSA PCSP.

(3) Information Systems With No Prior Accreditation. Information systems that required no previous accreditation must be certified and accredited in accordance with the NNSA PCSP.

5. REQUIREMENTS. Performance-Based Cyber Security Program. Performance-based approaches and other means must be used to evaluate and verify the effectiveness of cyber security measures, to identify areas requiring improvement, and to validate implemented improvements.

a. Protection Measures. Protection measures for all NNSA information systems must conform to the protection measures described in the NNSA PCSP, the element's CSPP, and the information system Security Plan.

b. Information Protection. As a minimum, the protection afforded information and the information system(s), on which it resides is based on a risk-based graded protection approach as defined by the NNSA PCSP.

(1) Protection measures may be strengthened based on an assessment of unique local threat(s) or the local evaluation of Consequence of Loss.

(2) All government information and any non-government information on an NNSA information system must be considered when determining the systems' protection measures.

c. Information Groups. NNSA information groups are the NNSA implementation of the DOE cyber security enclave classes. An information group contains all information that requires similar protection or is similar in content or use. All NNSA information must be identified as part of an NNSA approved information group. Attachment 3 contains the definition of NNSA information groups and the mapping between the information groups and DOE cyber security enclave classes.

d. Classified Information Access. Access to classified information must be granted only to persons with the appropriate access authorization and need-to-know in the performance of their duties according to NNSA policies and DOE O 472.1, *Personnel Security Program*.

e. Unclassified Information Access. Access to unclassified information must be granted to only those persons who have a need-to-know for the information in the performance of their duties. The individual disseminating the information is responsible for determining the recipients need-to-know in accordance with the Site's processes and NNSA policies and guidance.

f. Knowledge and Resources. All NNSA Federal and Contractor personnel must possess the knowledge, skills, equipment and resources to fulfill their cyber security responsibilities under both normal and emergency conditions.

g. Facility Clearance and Registration. NNSA elements with classified information systems must obtain prior approval through the Facility Clearance and Registration Process as outlined by NNSA NAPs and DOE O 470.1.

6. CONTACT. Questions concerning this NAP should be directed to the NNSA Cyber Security Program Manager at 202-586-4775.

7. DEFINITIONS. See Attachment 2.

8. IMPLEMENTED DOE CYBER SECURITY POLICIES. The NNSA PCSP implements the following DOE cyber security policies.

- P 205.1, Departmental Cyber Security Management Policy
- O 205.1, Department of Energy Cyber Security Management Program
- N 205.2, Foreign National Access to DOE Cyber Systems
- N 205.3, Password Generation, Protection, and Use
- N 205.4, Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents
- N 205.A, Certification and Accreditation Process for Federal Information Systems Including National Security Systems
- N 205.B, Cyber Security Requirements for Risk Management.

BY ORDER OF THE ADMINISTRATOR:

Linton Brooks
Administrator

Attachments

CHAPTER I

NNSA PCSP OVERVIEW

1. INTRODUCTION. This chapter provides a brief overview of the NNSA PCSP. The PCSP applies to any information system or network that is used to collect, create, process, transmit, store, or disseminate information for the NNSA. The NNSA PCSP implements national and departmental cyber security policies, including the International Standard Common Criteria Version 2.1, ISO IS 15408. The Common Criteria documents are available at http://csrc.nist.gov/cc/index.html.

2. PCSP MANAGEMENT. While cyber security is everybody's responsibility, there are several positions that have key roles in the NNSA PCSP. They are: 1) the Cyber Security Program Manager (CSPM), 2) the Designated Approving Authority (DAA), 3) a Cyber Security Office Manager (CSOM), 4) Cyber Security Site Manager (CSSM), 5) the System Owner, and 6) the Cyber System Security Officer (CSSO). The roles and responsibilities for these positions are described in Chapter II.

3. Cyber Security Program Plan. Implementation of the NNSA PCSP is documented in a Cyber Security Program Plan (CSPP). A CSPP must be prepared for each NNSA element and for NNSA enterprise major applications. The CSPP is the document that outlines the policies, procedures and practices of an element's cyber security program. The CSPP is a management level document and details the organization's policies, procedures and practices for ensuring effective cyber security. It also explains the site or application specific environment, missions and threats. The policies, procedures, practices, environments, missions, and threats for major applications are also documented in a CSPP.

4. Protection Profiles (PPs). Within the NNSA PCSP, information protection measures are graded according to the sensitivity of the information being protected. The NNSA PCSP identifies the protection measures according to information groups, ranging from Open Unrestricted Access up to Top Secret Restricted Data. The information groups are the NNSA implementation of DOE cyber security enclave classes. The minimum security functions and assurance measures are documented in PCSP PPs for each information group. The PPs are key components of the NNSA PCSP. A PP contains a set of security functions and assurance requirements taken from the Common Criteria or developed specifically by NNSA. A PP is a technology and implementation independent statement of security requirements for information with an identified sensitivity. The requirements in the PP are applied to products, a system(s), system of systems, or system components that will support the creation, processing, storing, display, or transmission of the information.

   The NNSA PCSP PPs provide a means of referring to a specific set of security needs and facilitates future evaluation against those needs. An NNSA PCSP PP can be developed by NNSA, by NNSA elements, by NNSA user communities, Information Technology product developers, or other organizations interested in defining such a common set of requirements.

The requirements in a PP must be implemented in an information system and documented in a Security Target (ST) as part of a System Security Plan. The ST specifies how the product or system achieves or implements the security requirements in a PP.

Figure 1 illustrates how PPs are applied to the protection of NNSA information and information systems. Figure 1 also illustrates how a standard NNSA PP can be adapted and applied, and the process for developing a new PP to meet unique technology or information protection needs.

5. Certification and Accreditation. The NNSA PCSP implements the national and departmental requirements for the Certification and Accreditation (C&A) of all information systems. The NNSA PCSP requires that each information system be accredited every three (3) years or when significant changes have been made in the information system, the information system environment, the threat, or cyber security requirements, (e.g., in response to changes in the NNSA PCSP). Each information system must receive an "accreditation" or an "interim approval to operate" before beginning operational activities. The process by which NNSA systems are Certified and Accredited is called the ISCAP – the NNSA Information Security Certification and Accreditation Process. The ISCAP is an integrated management process that involves the System Owner, the Designated Approving Authority (DAA), the CSOM acting on behalf of the DAA, the Cyber Security Site Manager (CSSM), and the Cyber System Security Officer (CSSO). The ISCAP establishes a standard NNSA approach to ensure a system (or group of systems) at a site is accredited to operate in a specified computing environment with an acceptable level of risk throughout its life cycle. The ISCAP activities standardize the C&A process to support a risk management focus on the mission, environment, and architecture for NNSA information systems.

6. System Security Plan. All systems processing information at a site must be included as part of a Systems Security Plan (SSP), also known as a Security Plan, and have received an “Accreditation” before being allowed to process information.

   The SSP is the basis for C&A of the system. The SSP documents the security environment in which the information system exists; the cyber security technical requirements (by incorporating the applicable STs) needed to protect the information on the system, and the conditions for C&A of the information system. The SSP is used throughout the entire C&A process to guide actions, document decisions, specify cyber security requirements, document solutions, and maintain operational systems security.

   The SSP can, and should be, tailored to address the characteristics of the information system, operational requirements, security policy, and prudent risk management throughout the system's life cycle as conditions change.

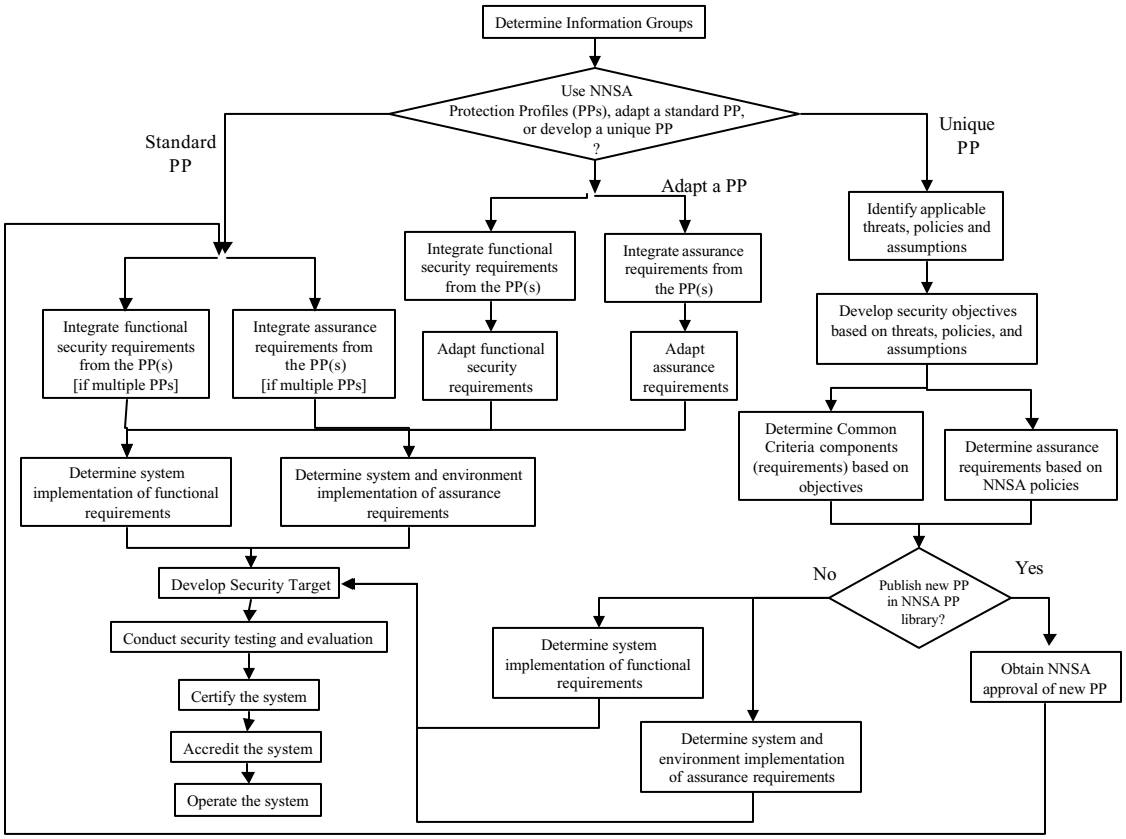

Figure 1. Application of PPs to NNSA Information Systems

This page intentionally blank.

CHAPTER II

MANAGEMENT STRUCTURE AND RESPONSIBILITIES

1. INTRODUCTION. The NNSA PCSP Cyber Security Program is managed through a multi-tiered structure. The structure includes a Cyber Security Program Manager (CSPM), Designated Approving Authorities (DAA), a Cyber Security Office Manager (CSOM), Cyber Security Site Managers (CSSM), and Cyber System Security Officers s (CSSO) at NNSA Headquarters; DAA(s), CSOM(s), CSSM(s), and CSSO(s) at the NNSA Service Center and NNSA Site Offices; and CSSMs, and CSSOs at contractor locations. The structure also includes NNSA Enterprise Major Application Program Managers, system owners, application owners, data owners, data stewards, and users of the systems. This chapter describes the roles and responsibilities of the individuals involved in the NNSA PCSP.

2. RESPONSIBILITIES.

   a. Administrator, National Nuclear Security Administration:

      (1) Assumes ultimate accountability for cyber security, and accepts the residual risk that exists within each of the NNSA elements through the approval of the NNSA PCSP.

      (2) Appoints the NNSA Cyber Security Program Manager who is the focal point for cyber security within the NNSA.

   b. Director, Office of Defense Nuclear Security:

      (1) Serves as the DAA for all information systems whose perimeter or presence as described in an SSP is wholly contained within the NNSA Headquarters Site and contractor or subcontractor facilities under the cognizance of the NNSA Administrator. The DAA approval authority may be delegated to another individual (who must be a Federal employee of the Office of Defense Nuclear Security or the Nuclear Safeguards and Security Program organization). All delegations by the Director, Office of Defense Nuclear Security must be documented in the NNSA Headquarters CSPP.

      (2) Approves the NNSA Headquarters CSPP. The CSPP approval authority may be delegated to another individual (who must be a Federal employee of the Office of Defense Nuclear Security or the Nuclear Safeguards and Security Program organization).

      (3) Approves Site Office and Service Center CSPPs. The CSPP approval authority may be delegated to another Manager (who must be a Federal employee of the Office of Defense Nuclear Security or the Nuclear Safeguards and Security Program organization).

(4) Ensures the appointment of a CSOM responsible for oversight of the implementation of the NNSA PCSP in the NNSA Headquarters and each contractor and subcontractor organization under the cognizance of NNSA Headquarters. The CSOM and DAA for NNSA Headquarters may be the same individual.

(5) Ensures the appointment of a CSSO for each information system in NNSA Headquarters.

(6) Ensures the appointment of a CSSM to be responsible for developing and implementing the CSPP in NNSA Headquarters.

(7) Ensures the appointment of a CSSM to be responsible for ensuring the development and implementation of the CSPP in each contractor and subcontractor organization under the cognizance of NNSA Headquarters.

(8) Ensures that all NNSA Headquarters personnel that use information systems and the information on the systems are aware of, and fulfill, their duties as described in the NNSA PCSP.

(9) Approves all NNSA CSPPs from contractor and subcontractors under the cognizance of NNSA Headquarters.

(10) Ensures that oversight reviews of all contractor and subcontractor sites (facilities) under the cognizance of NNSA Headquarters are conducted in accordance with the Survey (oversight) program defined in DOE O 470.1. Ensure that process/ program allowing access to information systems by Foreign Nationals is assessed as part of these reviews.

(11) Ensures that the NNSA PCSP is implemented in NNSA Headquarters;

(12) Ensures adequate resources are allocated to the Headquarters cyber security program;

(13) Ensures that the effectiveness of NNSA Headquarters cyber security is monitored through self-assessments and reviews.

(14) Ensures that NNSA Headquarters DAA, CSOM, CSSM, CSSO(s), Users, and System Administrators are trained in their specific duties and the technologies for which they have responsibilities.

c. Service Center Manager:

(1) Assume responsibility and accountability for the NNSA Service Center cyber security program.

(2) Serves as the DAA for all information systems whose perimeter or presence as described in an SSP is wholly contained (Federal or contractor) under the

cognizance of the NNSA Service Center. The Service Center Director/Manager's DAA Approval authority may be delegated to other employees of the Service Center or, through a memorandum of agreement, to NNSA federal employees at NNSA HQ or a Site Office.

(3) Appoint a CSSM responsible for oversight of the implementation of the NNSA PCSP in the Service Center and each contractor and subcontractor organization under the cognizance of the NNSA Service Center.

(4) Ensure the development and implementation of the CSPP in each contractor and subcontractor under the cognizance of the Service Center.

(5) Ensure that all personnel that use information systems and the information on the systems are aware of and fulfill their duties as described in the NNSA PCSP.

(6) Assumes responsibility and accountability for their organizations' cyber security programs;

(7) Ensures adequate resources are allocated to the Service Center cyber security program;

(8) Ensures the development, implementation, and maintenance of a CSPP for the Service Center;

(9) Ensures submission of the Service Center CSPP to the Director, Office of Defense Nuclear Security, for approval.

(10) Ensures the monitoring of cyber security effectiveness through self-assessments and reviews.

(11) Ensures that Service Center CSSM, CSSOs, Users, and System Administrators are trained in their specific duties and the technologies for which they have responsibilities.

d. Site Office Director/Manager:

(1) If the Site Office is not covered in another CSPP;

(a) Ensures the development, implementation, and maintenance of a CSPP for the Site Office;

(b) Submits the Site Office CSPP to the Director, Office of Defense Nuclear Security, for approval.

(1) Assumes responsibility and accountability for the Site Office cyber security programs;

(2) Serves as the DAA for all information systems whose perimeter or presence as described in an SSP is wholly contained within an NNSA Site (Federal or contractor) under the cognizance of the NNSA Site Office. The Site Office Director/Manager's DAA Approval authority may be delegated to other employees of the Site Office or, through a memorandum of agreement, to federal employees of another Site Office or the NNSA Service Center.

(3) Appoints a Cyber Security Office Manager (CSOM) responsible for oversight of the implementation of the NNSA PCSP in each NNSA element (including the Site Office) under the cognizance of the NNSA Site Office.

(4) Ensures the appointment of a CSSM to be responsible for developing and implementing the CSPP in the Site Office.

(5) Ensures the appointment of a CSSM to be responsible for developing and implementing the CSPP in each NNSA element under their cognizance.

(6) Ensures each information system in the Site Office has an appointed CSSO.

(7) Ensures that all Site Office personnel that use information systems and the information on the systems are aware of and fulfill their duties as described in the NNSA PCSP.

(8) Approves all NNSA CSPPs from NNSA elements under the cognizance of the Site Office Director/Manager.

(9) Ensures oversight reviews of all sites (facilities) under the cognizance of the Site Office Director/Manager are conducted in accordance with the Survey (oversight) program defined in NNSA policy. Ensure the process/ program allowing access to information systems by Foreign Nationals is assessed as part of these reviews.

(10) Ensures adequate resources are allocated to the Site Office cyber security program;

(11) Monitors effectiveness of cyber security through self-assessments and reviews.

(12) Ensures that Site Office DAA, CSOM, CSSM, CSSO(s), Users, and System Administrators are trained in their specific duties and the technologies for which they have responsibilities.

e. Contractors. The Laboratory Director or Production Facility Manager must:

(1) Assume responsibility and accountability for their organizations' cyber security program.

(2) Appoint a CSSM responsible for developing and implementing the NNSA PCSP at all facilities under the contract.

(3) Ensure the appointment of a CSSO for each information system managed or operated by the element.

(4) Ensure adequate resources are allocated to the element's cyber security program.

(5) Ensure that the effectiveness of the cyber security program is monitored through self-assessments and reviews.

(6) Ensure the development, implementation, and maintenance of the element CSPP.

(7) Submit the element CSPP to the cognizant Site Office for approval.

(8) Ensure the element's CSSM, CSSO, Users, and System Administrators are trained in their specific duties and the technologies for which they have responsibilities.

f. Cyber Security Program Manager. The CSPM must be a NNSA Federal employee, knowledgeable in cyber security. The CSPM must:

(1) Ensure the implementation of the NNSA PCSP.

(2) Serve as the NNSA primary point of contact for cyber security.

(3) Represent the NNSA PCSP before Federal, private, and public organizations concerned with protecting unclassified and classified government information.

(4) Serve as the DAA for all NNSA information systems or major applications with a perimeter or presence on different or multiple Sites. Hereafter, these information systems are called NNSA enterprise information systems or NNSA enterprise major applications. The NNSA CSPM DAA authority may be delegated to other NNSA Federal employees. All CSPM delegations must be documented.

(5) Approve NNSA Enterprise Major Application CSPPs. The CSPP approval authority may be delegated other NNSA Federal employees. All CSPM delegations must be documented.

(6) Develop, coordinate, disseminate, and maintain NNSA NAPs and guidance on all aspects of the NNSA PCSP, including cyber security, telecommunications security, TEMPEST, and Public Key Infrastructure (PKI) Programs.

(7) Annually review the NNSA Cyber Threat Statement, NNSA Cyber Threat Assessment, and NNSA PCSP.

(8) Ensure the development and maintenance of cyber security documentation for NNSA Enterprise systems.

(9) Establish and coordinate NNSA cyber security training, education, and awareness program.

(a) Ensure that education in NNSA's PCSP, policies, and practices is available to NNSA DAAs, CSOMs, CSSMs, CSSOs, and System Administrators within six (6) months of their appointment; and

(b) Periodically present cyber security workshops.

(10) Maintain a capability to facilitate the electronic exchange of information systems security information, such as awareness alerts on sniffer attacks, viruses, etc.

(11) NNSA INFOrmation CONdition (INFOCON).

(a) Evaluate NNSA computer network attack (CNA)/computer network exploitation (CNE) situations and recommend changes in NNSA INFOrmation CONdition (INFOCON) to the Chief, Office of NNSA Defense Nuclear Security.

(b) Notify NNSA elements, through the cognizant CSOMs, when the NNSA INFOCON is changed, through the most rapid means possible.

(12) Provide copies of approved CSPPs to other organizations, as required in NNSA policies.

(13) Coordinate with the DOE Office of Security, Office of Associate Chief Information Officer for Cyber Security, and Office of Independent Oversight and Performance Assurance on monitoring implementation of the PCSP through the joint review of selected implementation, self-assessment, and oversight documentation.

(14) Coordinate with the DOE Office of Intelligence on cyber security matters that affect SCI information systems at NNSA facilities.

(15) Identify NNSA cyber security resource requirements to ensure sufficient resources are planned and budgeted.

(16) Coordinate with the NNSA Chief Financial Office (CFO) and DOE CFO on budgets and expenditures related to NNSA cyber security.

(17) Monitor compliance and effectiveness of the PCSP through program reviews, budget reviews, self-assessments, management assessments, performance metrics analysis, and analysis of the results of peer reviews, vulnerability analysis, and independent oversight evaluations.

(18) Ensure the development and coordination of corrective actions plans involving NNSA enterprise systems in response to issues identified by the Office of Independent Oversight and Performance Assurance, peer reviews, and self-assessments.

(19) Manage a cyber security technology development program to support the NNSA PCSP, and periodically brief NNSA program managers, DAAs, CSOMs, and CSSMs on activities and results of the program.

(20) Approve secure remote diagnostic and maintenance facilities proposed for use with information systems that process classified information.

(21) Maintain and coordinate a NNSA cyber incident response capability to provide timely assistance and information system vulnerability information, cyber security incident response, watch and warning capabilities, analysis, and assistance reviews to all NNSA elements.

(22) Manage NNSA-wide cyber security incident reporting and response activities, in coordination with the DOE Office of Security, Office of Associate Chief Information Officer for Cyber Security, Office of Counterintelligence, or Office of Inspector General, as circumstances warrant.

(23) Coordinate with the DOE Office of Security and the DOE Office of Associate Chief Information Officer for Cyber Security on cyber security policy and the NNSA PCSP.

(24) Coordinate, as needed, with NNSA and DOE Offices of Counterintelligence (CN) on:

(a) Matters relating to policy and technical planning of CN activities.

(b) CN investigative activities.

(c) CN inspections, including evaluation of cyber security program components that affect CN programs, at NNSA facilities.

(d) Counterintelligence threat information.

(25) Coordinate with the Director of Intelligence on matters related to the cyber threat.

(26) Coordinate, as needed, with the DOE Office of the IG on IG investigation activities involving NNSA information systems.

(27) Report changes in CSOM and DAA appointments to all CSOMs and DAAs.

(28) Support, maintain, and coordinate an advice and assistance capability for use by any DAA, CSOM or CSSM within NNSA. This capability includes the reviews of information systems protection as requested by the element, such as review of network/system designs or PPs.

(29) Approve NNSA cyber security waivers and exceptions.

g. Designated Approving Authority. A DAA is an NNSA federal employee who is responsible for ensuring that all NNSA information systems under his / her cognizance are authorized to operate at an acceptable level of risk. The DAA:

(1) Approves the SSP required for each information system;

(2) Completes CSPM sponsored DAA training within six (6) months of assuming the DAA position.

(3) Ensures that each information system is certified that the protection measures documented in an SSP have been implemented and are functioning correctly. The DAA may designate additional tests that must be performed prior to accreditation;

(4) In accordance with the NNSA PCSP, formally approves the operation of the information system, grants an interim approval to operate (IATO), or declines to grant accreditation;

(5) Ensures that each information system is accredited or re-accredited every three (3) years (except for information systems that process Sensitive Compartmented Information) and that the accreditation or re-accreditation is documented.

(6) Withdraws accreditation to operate, or suspend operations if at any time

(a) Protection measures are no longer effective; or

(b) Changes are made to the operational environment, including changes in configuration, threat, changes to the classification or sensitivity of information on the system, connectivity, and/ or accepted risks that are no longer supported by the implemented protection measures.

(7) Approves changes in INFOCON requested by the NNSA element(s) under their cognizance.

(8) Ensure the completion of all activities defined for the Information System Certification and Accreditation Process (ISCAP).

h. Cyber Security Office Manager. The Cyber Security Office Manager (CSOM) is an NNSA Federal employee, knowledgeable in information systems security, and appointed by the Site Office or Service Center Director/Manager. The CSOM must:

(1) Communicate appropriate incident reports received from NNSA elements to the CSPM.

(2) Report changes in NNSA INFOCON to all NNSA elements and DAAs under his/ her cognizance, through the most rapid means available.

(3) Report changes in the local INFOCON status of NNSA element(s) to the NNSA CSPM.

(4) Ensure periodic review of the PCSP implementation, consistent with the NNSA Office Survey Program, at each element under the cognizance of the NNSA Site Office.

(5) Monitor responses to findings and other deficiencies identified in surveys, inspections, and reviews of each element under the cognizance of the NNSA Site Office to ensure that any necessary corrective or compensatory actions have been completed.

(6) Participate in CSPM sponsored cyber security training within six (6) months of his / her appointment

(7) Coordinate element requests for advice and assistance services provided by the CSPM.

(8) For NNSA sits, with SCI information systems:

(a) Review SSPs and provide recommendations to the DOE Office of Intelligence;

(b) Review certifications for SCI information systems and provide accreditation recommendations to the DOE Office of Intelligence.

i. Cyber Security Site Manager. The CSSM is appointed by the NNSA element manager to be responsible for development of the element's CSPP and implementation of the element's cyber security program. A separate CSSM may be appointed for information systems in a SCIF if the element determines that another CSSM is needed. In this capacity, the SCIF CSSM also functions as the element point of contact (POC) for all information systems security issues in the SCIF(s).

(1) Maintains record copies of the element's CSPP and ensures that a record copy of each SSP is maintained.

(2) Ensures each CSSO and system administrator is aware of and fulfills his/ her cyber security duties as described in the PCSP and the element's CSPP.

(3) Ensures the development, documentation and presentation of information systems security education, awareness, and training activities for element management, cyber security personnel, application owner, data steward, and users.

(a) Ensures that users are trained on the information systems cyber security features, operation, and safeguards prior to being allowed access to the system.

(b) Ensures that CSSOs and systems administrators are trained on information systems cyber security requirements, operations, and safeguards.

(4) Establishes, documents, and monitors the element's cyber security program implementation and ensures element compliance with the NNSA PCSP. Upon completion of each assessment or review, the CSSM must ensure that a corrective action plan is prepared and implemented for all findings or vulnerabilities as directed by DOE O 470.1. A record of each review and the subsequent corrective action plan must be retained and made available during future surveys and inspections.

(5) Identifies and documents, in coordination with the organization's Operations Security (OPSEC) program, element-specific threats to information systems and information at the Site.

(a) Develops and documents additional or modified protection measures for those threats.

(b) Obtains approvals for the modified protection measures from the cognizant DAA.

(6) Ensures the CSPP is coordinated with other Site Plans/ Programs to include: Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP), Classified Matter Protection and Control, Physical Security, Personnel Security, Telecommunications Security, TEMPEST, Technical Surveillance Countermeasures, Operations Security, and Nuclear Materials Control and Accountability.

(7) Ensures the development of procedures to implement the element's cyber security program on all information systems.

(8) Certifies to the cognizant DAA that the protection requirements described in the SSP for each information system have been implemented and are operational as required in Chapter VII of this document.

(9) Ensures that the cognizant DAA is notified when the information system is no longer needed or when changes occur that might affect the accreditation of the information system.

(10) Participates in CSPM sponsored cyber security training within six (6) months of his/ her appointment.

(11) Ensures the development, documentation, and presentation of cyber security training for escorts in information systems operational areas.

(12) Ensures that each information system user acknowledges, in writing or electronically using NNSA-approved digital signature technologies, his/ her responsibility (Code of Conduct) for the security of information systems and information;

(13) Communicates incident reports to the CSOM.

(14) Establishes and conducts the NNSA element's peer review process.

(15) Conducts self-assessments in accordance with NIST 800-26.

(16) Ensures each individual responsible for major applications within the NNSA element is aware of and fulfills his / her cyber security duties as described in the PCSP and the element's CSPP. A major application manager:

(a) Assumes responsibility and accountability for the major application's cyber security implementation;

(b) Ensures adequate resources are allocated to the major application's cyber security implementation;

(c) Monitors the effectiveness of the major application's cyber security through self-assessments and reviews;

(d) Ensures the development and maintenance of the major application Security Plan;

(e) Coordinates the SSP with the involved NNSA element managers.

(17) Recommend changes in the NNSA element INFOCON status.

j. Information System Owner. The information system owner is the person or organization that is responsible for acquiring, operating or upgrading an information system. The System Owner coordinates all aspects of the system for

which he or she is responsible from initial concept, through development, to implementation and system maintenance. The Information System Owner:

(1) Ensures the preparation of the SSP and development of all supporting PP and ST.

(2) Ensures the certification and accreditation all information system(s) under his / her cognizance.

k. Enterprise Major Application Program Manager. The NNSA Enterprise Major Application Program Manager is the person or organization that is responsible for acquiring, operating or upgrading an NNSA Enterprise Major Application and is responsible for the application configuration at all NNSA elements. The NNSA Enterprise Major Application Program Manager:

(1) Assumes responsibility and accountability for the application's cyber security;

(2) Ensures adequate resources are allocated for the application's cyber security;

(3) Monitors the effectiveness of the application's cyber security through self-assessments and reviews;

(4) Ensures the development and maintenance of the Enterprise Major Application SSP and supporting PPs and STs;

(5) Coordinates the SSP with the involved NNSA element managers.

(6) Ensure the development and maintenance of the Enterprise Major Application CSPP.

(7) Coordinates the Enterprise Major Application CSPP with the involved NNSA element managers.

(8) Submits the Enterprise Major Application CSPP to the CSPM for approval.

(9) Ensures the involved NNSA elements' CSSM, CSSO, Users, and System Administrators involved with the Enterprise Major Application are trained in their specific duties and responsibilities with respect to the Enterprise Major Application

(10) Maintains a record copy of the Enterprise Major Application CSPP and ensure that a record copy of the SSP is maintained.

(11) Ensures the distribution, as needed, of the Enterprise Major Application CSPP and SSP to other NNSA elements

l. Cyber System Security Officer. The following roles and responsibilities apply to all information system for which the CSSO is responsible. Multiple information systems may be assigned to a single CSSO.

(1) Ensures the implementation of protection measures that are documented in the SSP for each information system for which he / she is the CSSO.

(2) Ensures that privileged users are granted access to information system's resources based on the least privilege principle.

(3) Identifies, in coordination with the CSSM, and documents in the Security Plan, unique threats to information systems for which he/ she is responsible.

(4) Ensures that the confidentiality, integrity, and availability sensitivity levels of the information are determined prior to use on an information system.

(5) Documents any special protection requirements identified by the application owner, data owner, or data steward and ensure that these requirements are included within the protection measures implemented in the information system.

(6) Ensure each information system for which he / she is the CSSO is covered by a Security Plan.

(7) Maintains a record copy of the SSP for each information system for which he / she is the CSSO.

(8) Ensure the implementation of element procedures defined in the element CSPP and the SSP for each information system for which he / she is the CSSO.

(9) Ensures that the cognizant CSSM is notified when an information system is no longer needed or when the changes occur that might affect the accreditation of the information system.

(10) Ensures that information access controls and cyber protection measures are implemented for each information system as described by its Security Plan.

(11) Ensures that users and systems administrators are properly trained in information system security by identifying cyber security training needs and the personnel who need to attend the cyber security training program.

(12) Conducts cyber security reviews and tests to ensure that the cyber security features and controls are functioning and effective.

(13) Participates in the CSSM's self-assessment and training program.

(14) Ensures the performance of a risk assessment to determine if additional countermeasures beyond those identified in the SSP are required, if directed, and/or if an identified unique local threat exists.

(15) Communicates incident reports to the CSSM.

(16) Ensures the implementation of all applicable protection measures for each information system.

(17) Conducts cyber security reviews and tests to ensure that the protection features and controls are functioning and effective.

(18) Ensures that unauthorized personnel are not granted use of, or access to, the information system.

m. Application Owners/ Data Owners / Data Stewards. These roles and responsibilities apply to all information systems.

(1) Determine and declare the sensitivity of the information prior to the information being created, processed, stored, transferred, or accessed on the information system.

(2) Identify and document unique threats to their information.

(3) Advise the CSSO of any special confidentiality, integrity, or availability protection requirements for the information.

(4) Ensure that the information is processed only on a system that is approved at a level to protect the information.

(5) Determine and document the data and application(s) that are essential to fulfill the organizational mission (identify major applications) and ensure that requirements for contingencies are determined, implemented, and tested.

n. Users. The roles and responsibilities apply to all cyber assets.

(1) Comply with the requirements of the NNSA PCSP, the NNSA element's CSPP, and the information system Security Plan.

(2) Be aware of, and knowledgeable about, their responsibilities in regard to information systems security.

(3) Ensure that any authentication mechanisms (including passwords) issued for the control of their access to information on information systems are not shared and are protected at the same level of protection applied to the information to which it permits access, and report any compromise or suspected compromise of an authenticator to the appropriate CSSO.

(4) Be responsible and accountable for their actions on an information system.

(5) Acknowledge, via NNSA-approved electronic signature or in writing, their responsibilities (Code of Conduct) for protecting information systems and classified information.

(6) Participate in training on the information system's prescribed security restrictions and safeguards before initial access to a system. As a follow-up to this initial training, participate in an ongoing security education, training, and awareness program.

(7) Immediately report all security incidents and potential threats and vulnerabilities involving the information system to the appropriate CSSO;

(8) Ensure that system media and system output are properly classified, marked, controlled, and stored;

(9) Protect terminals from unauthorized access as described in the information system Security Plan;

(10) Inform the CSSO when access to a particular information system is no longer required (e.g., completion of a project, transfer, retirement, resignation);

(11) Observe rules and regulations governing the secure operation and authorized use of information systems; and

(12) Use the information system only for official Government business or other activities authorized by NNSA or the NNSA element manager.

(13) Receive electronic or written permission from the CSSM before any attempt to bypass, strain, or test security mechanisms; any ongoing or regular bypass of security mechanisms must be approved by the cognizant DAA;

(14) Privileged Users.

(a) The number of privileged users must be limited to the minimum number needed to manage the system.

(b) All privileged users must be responsible for all requirements stated for general users.

(c) Privileged users are responsible to ensure that user access to the information system’s resources and information is based on the least privilege principle.

(d) All privileged users must

i. Be U.S. citizens, unless otherwise approved in accordance with the approved NNSA element CSPP or in writing by the cognizant DAA;

ii. Possess approvals of need-to-know for all information on the system;

iii. Possess an Access Authorization sufficient for clearance equal to the highest classification and most restrictive category of data processed on the information system;

iv. Use unique identifiers as described in the information system Security Plan;

v. Protect the root or super-user authenticator at the highest level of data it secures;

vi. Be responsible for all super-user or root actions under his/her account;

vii. Report any and all security relevant information system problems to the CSSO; and

viii. Use the special access or privileges granted only to perform authorized tasks and functions.

o. Director of NNSA Counterintelligence.

(1) Coordinates all investigative issues concerned with the PCSP with the NNSA CSPM.

(2) Coordinates with the NNSA CSPM when conducting and coordinating investigations of intrusions and anomalous activity into NNSA information systems.

(3) Coordinates inspection schedules with the NNSA CSPM on all independent inspection of counterintelligence programs that include the evaluation of NNSA cyber security program components that affect CN programs.

(4) Provides counterintelligence support to the NNSA CSPM, DAAs, CSOMs, and CSSMs.

(5) Provides relevant threat information to the NNSA CSPM.

p. Director, DOE Office of Intelligence.

(1) Coordinates all investigative issues concerned with the NNSA PCSP and related to SCI information systems located on NNSA facilities with the NNSA CPSM.

(2) Coordinates inspection schedules with the NNSA CPSM on inspections of SCI information systems located on NNSA facilities.

q. Office of the Inspector General.

(1) Coordinates all investigative issues concerned with the PCSP with the NNSA CSPM.

(2) Coordinates with the NNSA CSPM when conducting and coordinating investigations of intrusions and anomalous activity into NNSA information systems.

(3) Provides relevant criminal threat information to the CSPM to assist in the development, improvement, and maintenance of the PCSP.

CHAPTER III

RISK AND PROGRAM MANAGEMENT

1. INTRODUCTION. The cornerstone of the NNSA PCSP is the risk management process, which determines the protection requirements for NNSA information and the computing resources used to collect, create, process, transmit, store, or disseminate information. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. The objective of performing risk management is to enable the organization to accomplish its mission(s) (1) by better securing the information systems that collect, create, process, store, or transmit information; (2) by enabling management to make well-informed risk management decisions to justify the expenditures; and (3) by assisting management in approving information systems on the basis of the supporting documentation resulting from the performance of risk management. Risk management is the process that allows managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the information systems and data that support their organizations' missions.

2. RISK MANAGEMENT PROCESS. NNSA's risk management process includes the following interrelated phases:

   a. System Characterization. The boundaries of the information system are identified, along with the resources and the information that constitute the system.

   b. Threat Analysis. The NNSA Cyber Threat Statement identifies the threats to NNSA cyber systems and the NNSA Cyber Risk Assessment provides an assessment of the risks posed by the cyber threats to NNSA information systems and assets.

   c. Vulnerability Identification. The analysis of the threat to an information system must include an analysis of the vulnerabilities associated with the system environment.

   d. Analysis of Protection Measures. The goal of this step is to analyze the protection measures that have been implemented, or are planned for implementation, to minimize or eliminate the likelihood (or probability) of a threat's exploiting a system vulnerability. The NNSA PPs identify the minimum protection measures that must be applied to NNSA information systems and assets. Other protection measures are documented in the NNSA PCSP and must be applied to NNSA information systems and assets.

   e. Likelihood Determination. The NNSA Cyber Risk Assessment provides an assessment of the likelihood of occurrence of cyber threats to NNSA information and information technology systems.

f. Risk Determination. This step assesses the level of risk to the information system by evaluating:

- NNSA Cyber Threat Statement and the results of the NNSA Cyber Risk Assessment;
- Adjustments, if any, to the NNSA specified Consequence of Loss of confidentiality, integrity, and availability for the information assets to be stored, processed, or transmitted on the system;
- Data steward declarations of Consequences of Loss of confidentiality, integrity, and availability that exceed NNSA determination for the information assets;
- Information system protection measures and architectures; and
- CSPP implementation that evaluates the unique concerns of the element (i.e., threats, protective technologies, procedures, etc.).

g. Protection Measure Recommendations. The NNSA cyber security process includes the identification of a PP that results in the identification of the minimum protection measures that must be applied to the information system. If the risk assessment process determines that additional protection measures are appropriate, the following factors should be considered in recommending protection measures and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability.

h. Risk Mitigation. Risk mitigation, the second component of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing protection measures developed during the risk assessment process. Risk mitigation can be achieved through any of the following risk mitigation options:

(1) Risk Assumption. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk.

(2) Risk Avoidance. To avoid the risk by eliminating the risk cause and/or consequence (e.g., forego certain functions of the system or shut down the system when risks are identified).

(3) Risk Limitation. To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls).

i. Protection Measure Implementation. Protection measures, identified in the PP or ST, are implemented by addressing the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities. The following risk mitigation methodology describes the approach to control implementation:

- Evaluate Recommended Protection Measure Implementation Options. During this step, the feasibility (e.g., compatibility, user acceptance, cost) and effectiveness (e.g., degree of protection and level of risk mitigation) of possible protection measure implementation approaches are analyzed. The objective is to select the most appropriate protection measure implementation option for minimizing risk.
- Select Protection Measure Implementation. On the basis of the results of the cost-benefit analysis, management determines the most cost-effective implementation approach for measures(s) to reduce risk to the organization's mission. The implementation approaches selected should combine technical, operational, and management elements to ensure adequate security for the information system and the organization.
- Conduct Cost-Benefit Analysis. To allocate resources and implement cost-effective protection measures, organizations, after evaluating the feasibility and effectiveness of the identified possible protection measures, should conduct a cost-benefit analysis for the implementation of each proposed measure to determine which approaches are required and appropriate for the information system. In all cases, the minimum protection requirements in the NNSA PCSP must be implemented prior to system operation.
- Develop the Security Plan.
- Implement Protection Measures(s). Depending on individual situations, the implemented measures may lower the risk level but not eliminate the risk.

j. Residual Risk. Organizations can analyze the extent of the risk reduction generated by the new or enhanced protection measures in terms of the reduced threat likelihood or Consequence of Loss impact, the two parameters that define the mitigated level of risk to the organizational mission. Implementation of new or enhanced measures can mitigate risk by eliminating some of the system's vulnerabilities (flaws and weakness), thereby reducing the number of possible threat-source/vulnerability pairs or adding a specific protection measure to reduce the capacity and motivation of a threat-source.

k. System Operation. The final phase of the risk management process is acceptance of risk through C&A and the protection of information during day-to-day operations.

l. Evaluation And Assessment. In most organizations, the network/system itself will continually be expanded and updated, its components changed, and its

software applications replaced or updated with newer versions. In addition, personnel changes will occur and security policies are likely to change over time. These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving.

CHAPTER IV

CONSEQUENCE OF LOSS

1. . The levels of Consequence of Loss reflect the sensitivity of the information and the consequences of the loss of confidentiality, integrity, and availability. The levels of consequence must be considered when determining which security measures should be required of networks and multi-user information systems. NOTE: The Consequence of Loss of confidentiality, integrity, and availability are used to develop or modify a PP or ST for an information system.

2. Determination of Level of Consequences. The Consequence of Loss definition matrices, **Table 1** through **Table 3**, assist in determining the appropriate technical requirements needed to meet the NNSA security objectives of confidentiality, integrity, and availability. The Consequence of Loss tables should be used as follows:

   - A determination for a Level of Consequence of very high, high, medium, low, or very low must be made for each of the three objectives: confidentiality, integrity, and availability. *The Level-of-Consequences rating is independent for each of these objectives*.
     - Consequence Of Loss Of Confidentiality. In considering confidentiality, the principle question is the necessity for preventing unauthorized disclosure of information on the information system.
     - Consequence Of Loss Of Integrity. In considering integrity, the principal question is the necessity for preventing unauthorized modification of the information on the information system.
     - Consequence Of Loss Of Availability. In considering availability, the principal consideration is the need for the information on the information system to be available in a fixed time frame to accomplish its mission.
   - NNSA has assigned minimum levels of consequence for each information group, **Table 4**, based on the definitions of consequence of loss of confidentiality, integrity, and availability in, Table 1, **Table 2**, and **Table 3**. The levels of consequence in Table 4 are minimum values. Additional data owner or data steward protection requirements for an information group may require a level of consequence greater than the NNSA assigned minimum.

Table 1. Consequence of Loss of Confidentiality

Consequence Of Loss	Confidentiality
Very High	• Grave damage to national security will result if confidentiality is lost; or • Information designated as life- or mission-critical;
High	• Unauthorized, premature, or incomplete disclosure may have an adverse effect on national security, NNSA, DOE, or national interests.
Medium	• Serious damage to national security will result if confidentiality is lost; • Information requiring protection mandated by policy, laws, or agreements between NNSA, its contractors, and other entities, such as DOE, commercial organizations or foreign governments; or • Information designated as mission-essential; or • Unauthorized, premature, or incomplete disclosure may have an adverse effect on site-level interests.
Low	• Damage to national security will result if confidentiality is lost; • Information designated as sensitive by the data owner; or; • Unauthorized, premature, or incomplete disclosure may have an adverse effect on organizational interests.
Very Low	• No damage to national security; • Information essentially requires no protection against disclosure.

Table 2. Consequence of Loss of Integrity

Consequence Of Loss	Integrity
Very High	• Grave damage to national security will result if integrity is lost; or • Information designated as life- or mission-critical; or
High	• Loss of integrity will have an adverse effect on national-level interests; • Loss of integrity will have an adverse effect on confidentiality.
Medium	• High degree of integrity required for mission accomplishment, but not absolute; or • Bodily injury might result from loss of integrity; or • Loss of integrity will have an adverse effect on organizational-level interests.
Low	• Loss of integrity impacts only the mission(s) of site- or office-level organization.
Very Low	• Loss of integrity has little or no impact on any level of organization in the NNSA and its contractors.

Table 3. Consequence of Loss of Availability

Consequence Of Loss	Availability
High	• Loss of life might result from loss of availability; • Information must always be available upon request, with no tolerance for delay; or • Loss of availability will have an adverse effect on national-level interests; • Federal requirement (i.e., requirement for MC&A inventory); or • Loss of availability will have an adverse effect on confidentiality.
Medium	• Information must be readily available with minimum tolerance for delay; or • Bodily injury might result from loss of availability; or • Loss of availability will have an adverse effect on organizational-level interests.
Low	• Information must be available with flexible tolerance for delay.
Very Low	• Information availability is a low priority for system mission.

Note: In this context, “High – no tolerance for delay” means no delay; “Medium – minimum tolerance for delay" means a delay of seconds to hours; and “Low – flexible tolerance for delay” means a delay of days to weeks

Table 4. Consequence of Loss of Confidentiality, Integrity, and Availability

Information Group			Loss of Confidentiality	Loss of Integrity	Loss of Availability
Open, Public Unrestricted Access			Very Low	Low	Very Low
Unclassified Protected			Low	Very Low	Very Low
Unclassified Mandatory Protection			Medium	Low	Very Low
Confidential Non-Nuclear Weapons			Medium	Very Low	Very Low
Secret Non-Nuclear Weapons			Medium	Very Low	Very Low
Confidential Nuclear Weapons Data	Sigma	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, and 13	High	Low	Very Low
Secret Nuclear Weapons Data	Sigma	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, and 13	High	Low	Very Low
		14 and 15	Very High	Low	Very Low
Top Secret			Very High	Low	Very Low
Top Secret Restricted Data			Very High	Low	Very Low
Special Information Group			TBD	TBD	TBD

NOTE: The levels in this table are the minimum values allowed by NNSA. NNSA Program Managers or Data Stewards may assign a higher level of consequence for any or all of the information groups. See Attachment 3 for a description of each Information Group.

CHAPTER V

CYBER SECURITY MEASURES

1. INTRODUCTION. Cyber security objectives for the NNSA PCSP are:

   - Confidentiality. Assurance that information is not disclosed to unauthorized persons, processes, or devices.
   - Availability. Timely, reliable access to data and information services for authorized users.
   - Integrity. Protection against unauthorized modification or destruction of information.

   a. Cyber Security Principles. The NNSA cyber security objectives are accomplished though application of the following cyber security controls called cyber security principles. Each NNSA information system must apply the following principles by implementing the minimum protection objectives defined for each information group on the information system.

   - Access Control. Limit access to information system resources only to authorized users, programs, processes, or other information systems.
   - Alternate Infrastructure. Users have continuing access, in accordance with mission need, to information and the information systems used to process the information.
   - Audit. Capture data pertaining to the accessing of information system resources, make data available for review, and maintain data in a secure state.
   - Authentication. Verify a user's identity prior to granting access to system resources.
   - Composability. When systems are composed of other systems to create a larger system environment, boundary protection and allocation of security controls must provide the appropriate security functionality and assurances to protect each component system and the combined system as a whole. This includes the use of controlled interfaces to ensure boundary protection.
   - Configuration Management. Protection features are maintained in the information system by applying a level of discipline and control to the process of system maintenance and modification.
   - Continuity of Operations. Provide for response, recovery and the return to normal operations in the event of failure in an information system.
   - Controlled Interfaces. Measures applied to monitor and enforce the protection requirements of interconnected networks and to adjudicate security policy differences between networks.

- Cryptographic Services and Data Transmission Security. Ensure that the confidentiality of the information is protected in unsecured environments and protect against interception, replay, and insertion of data as it is transmitted.
- Data Assurance. Detect, deter, or prevent changes to data.
- Data Backup And Restoration. Ensure data is available when needed.
- Education and Awareness. Provide education and awareness in cyber security vulnerabilities, threats, protection strategies, and organizational/personal responsibilities.
- Entity Integrity. Ensure the protection of data and software stored or transmitted internally within the system.
- Forensics. Identify, collect, and preserve to allow reconstruction and analysis after cyber attacks, failures, and misuse.
- Intrusion Detection and Response. Detect and respond to unauthorized attempts to penetrate the system and respond to detected incidents
- Least Privilege. Grant the most restrictive set of privileges needed for the performance of authorized tasks.
- Life-Cycle Management. Manage changes to security critical components throughout the system lifecycle.
- Malicious Code Detection. Protect the information system against software or firmware designed to adversely impact the information, the information system, or the operation of the system.
- Marking and Review. Ensure that the sensitivity of information is unambiguously associated with the written or electronic representation of the information.
- Personnel Security. Personnel with system access play an integral role in protecting information, defining system security policies, and maintaining and monitoring the confidentiality, integrity, and availability attributes that are inherent within the information systems.
- Physical Security. The information and information system resources are protected in controlled access facilities that mitigate unauthorized, physical access.
- Risk Assessment. Assess the impact of threats to resources by the exploitation of vulnerabilities and to identify cost-effective countermeasures to reduce risks to an acceptable level.
- Residual Information Protection. Ensure that a resource (logical or physical) does not contain residual data prior to the resource being made available to other entities or environments.
- Secure System Management, Control, and Operation. Ensure the management, control and operation of security critical functions of the information system.

- Session Control. Measures, over and above identification and authentication, for the establishment of a secure user session.
- System Assurance. Assurance that the security critical components of an information system are able to protect themselves from unauthorized access.
- System Recovery. Restoration of a system to a secure state after a failure or interruption of service.
- Testing. Exercising and evaluating the operation of the system.
- User Identification. Identify users prior to granting access to information through system resources.
- Waste, Fraud, and Abuse Protection. Detect, prevent and report waste fraud and abuse in accordance with NNSA policies and site procedures.

The NNSA cyber security principles are accomplished through mechanisms or procedures called cyber security measures. A single measure may be used to support multiple principles and multiple measures may be needed to support all aspects of a principle.

Following the description of each measure are the NNSA cyber security policy statements that express the measure as an NNSA policy that must be addressed in construction of NNSA-specific PPs. The policy statements are expressed in a PP using Common Criteria notation, e.g., an identifier (e.g., P. Audit), the policy statement, and additional explanatory comments.

2. CYBER SECURITY MEASURES.

a. Access Controls. Measures designed to limit access to information system resources to authorized users, programs, processes, or other systems and to manage authorities and privileges granted to each user of the information system or application. These measures must include maintenance of 1) the association between a user identifier and an authenticator; 2) user authorizations and privileges; 3) user access to objects; 4) authority to grant access to objects and subjects, and 5) authority to modify objects and subjects. This measure supports the Access Controls and Least Privilege principles.

P.LEAST_PRIV	Privileges granted to information system users (including privileged users) are the most restrictive (least privilege) set of privileges needed for the performance of authorized tasks.
P.NTK	Access to data in information system resources is limited to users with the need-to-know for the information, regardless of the form of the information. Access rights to specific data objects are determined by object attributes assigned to that object, user identity,

user attributes, and environmental conditions as defined by the security policy.

b. Alternate Infrastructure. Measures to ensure that users have continuing access, in accordance with mission need, to information and information systems used to process the information. An alternate infrastructure can also provide time for orderly system shutdown or the transfer of system operations to another system or power source. This measure supports the Alternate Infrastructure and Continuity of Operations principles.

P.ALT_INFRASTRUCT	Information system users have, based on mission need, continuing access to the information system hardware and software assets.

c. Audit. Measures to collect, review, reduce, analyze, protect, archive, and generate reports on accesses to system resources, use of privileges, and changes in system state. The information system will create, protect, and maintain a file(s), typically called an audit log or file, for recording security relevant events. This measure supports the Audit principle.

P.ACCOUNTABILITY	Users are held accountable for their actions, and actions taken on their behalf, on the information system.
P.MONITORING	All users activities, and activities on behalf of the user, are monitored and reviewed for activities that are detrimental to the confidentiality, integrity or availability of the information or information system.

d. Authentication. Measures used to unambiguously verify a user's identity prior to granting access to system resources. Users are required to authenticate their identity at logon time by presenting a password or other approved authenticator to the system. The authentication process must be successfully completed prior to user access to information, or executing of any application, utility, etc. on the system. This measure supports the Identification and Authentication principles.

P.AUTH_MGMT	The process of generating, issuing, and using authenticators is managed in accordance with NNSA and site policies.
P.KNOWN	All NNSA multi-user information systems, desktops, and laptops– excluding those information systems intended to provide public access (e. g., public web servers)– must have, and use, a mechanism that authenticates the identity of each person before providing access to any information system, application, service or resource.

P.CREDENTIAL_PROTECTION Authentication credentials shall be protected to prevent unauthorized access, modification or destruction. This policy requires that the individuals and IT entities that use the credentials adequately protect all credentials. The information system supports this policy by restricting access to credentials, by protecting the credentials as they are transmitted over the network during the domain authentication process, and through the trusted path between the credential reader and other information system components.

P.AUTHENTICATION All users shall be authenticated prior to being granted access to systems and the information and resources managed by those systems.

P.STRONG_AUTHENTICATION All users shall be authenticated by two-factor strong authentication mechanisms prior to being granted access to systems and the information and resources managed by those systems.

e. Composability. Measures used to assure that when systems are combined to create larger systems the security of the collective whole does not unaccountably deteriorate from that of any individual system. A review process must be implemented to ensure the combined system does not increase the level of risk accepted by the Designated Approving Authority (DAA) for the individual systems. This measure supports the Composability principle.

P.COMPOSITION The security of an information system or network composed of individual information systems is equal to or greater than that of any individual system in the combined system.

f. Configuration Management. Measures to ensure the protection features are maintained in the system by applying a level of discipline and control to the process of system maintenance and modification. A configuration management process must be implemented to detect any changes in system hardware, software, and firmware components that will modify the level of risk accepted by the DAA. This measure supports the Configuration Management, Life Cycle Management, and Security System Management, Control and Operation principles.

P.CONFIG_MGMT Protection features of a system are maintained during development, installation, modification, and maintenance of the hardware, firmware, and software components.

g. Controlled Interface. Measures applied to monitor and enforce the protection requirements of interconnected networks and to adjudicate security policy

differences between the networks. These measures include secure interconnections that adjudicate differences in security policy to enable or prohibit the flow of information between interconnected automated information systems operating under different security policies. Controlled interface measures include providing a secure point of interconnection between networks, connected peripheral devices, remote terminals, or remote hosts; provide a reliable exchange of security-related information; and providing filtering of information in a data stream based on security labels. This measure supports the Composability and Controlled Interface principles

The controlled interface may be approved by the DAA as a separate system or considered a component of the network with the more restrictive cyber security policy or whose information loss of confidentiality has the highest level of consequence.

P.CTL_INTERFACE	Protection requirements and adjudication of security policy differences are enforced when two or more information systems or networks are interconnected.

h. Continuity of Operations. The requirements for continuity of operation of mission essential applications, data, and information systems must be reviewed and identified. The decision regarding the need for a contingency or continuity of operations plan must be documented in the information system Security Plan. If a contingency plan or continuity of operations plan is needed, the plan must be developed and incorporated into the Security Plan. This measure supports the Continuity of Operations principle.

P.CONOPS	Continuity of operations planning is applied to mission essential applications, data, and information systems.

i. Cryptographic Services and Data Transmission Security. Measures to ensure that the confidentiality of the information is protected in unsecured environments. Communications security controls protect against interception, replay, and insertion of data as it is transmitted. Encryption mechanisms and supporting controls (e.g., key management) are central to communications security, but can also be used to protect stored information. This measure supports the Access Controls, Cryptographic Services and Data Transmission Security, and Entity Integrity principles.

NNSA approved Protected Transmission Systems, NSA approved cryptographic services, or NNSA approved cryptographic services are employed where information is being placed in, or transmitted through, an environment that cannot provide the protection or need-to-know separation required by the PCSP or Site policies.

P.CRYPTOGRAPHY	Cryptographic services that are used to ensure information confidentiality, privacy or integrity shall

meet the criteria of the appropriate robustness (strength of mechanism and assurance) based on the sensitivity of information to be protected and the threat environment.

j. Data Assurance. Measures to ensure data integrity. As required by the PP, NNSA policy, or data owner/steward, the information system must be able to detect, deter, or prevent changes to data. A transaction log, protected from unauthorized changes, may be necessary to allow immediate correction of unauthorized data changes and for the off line verification of all changes. This measure supports the Data Assurance, Entity Integrity, and Least Privilege principles.

P.DATA_ASSURANCE Modification of data is permitted only by authorized personnel or processes.

k. Data Backup and Restoration. Measures to ensure that user and system data are available, or restorable, when needed. This measure supports the Data Assurance, Data Backup and Restoration, and Continuity of Operations principles.

P.DATA_AVAILABILITY User and information system data are available, or restorable, to meet mission availability requirements

l. Education and Awareness. Ensure all members of the organization receive sufficient training, and that the training is refreshed, annually. This measure supports the Education and Awareness principle.

Once granted legitimate access, authenticated users are expected to use information system resources and information only in accordance with the organizational security policy. In order for this to be possible, these users must be adequately trained both to understand the purpose and need for security controls and to be able to make secure decisions with respect to their discretionary actions.

Authenticated users of the system must be adequately trained, enabling them to (1) effectively implement organizational security policies with respect to their discretionary actions and (2) support the need for non-discretionary controls implemented to enforce these policies prior to being granted access to information.

P.TRAINING All users are trained to understand applicable system-use policies, the proper use of systems and the vulnerabilities inherent to those systems. This policy ensures that all users are properly instructed on policies and procedures for using the system as well as being able to acknowledge all threats and vulnerabilities that may impact system processing.

m. Forensics. Measures to identify, collect, and preserve information needed for reconstruction after a penetration and analyze on-going or past cyber attacks and

failures. This measure supports the Forensics and Intrusion Detection and Response principles.

P.FORENSICS	Information needed for penetration reconstruction, and analyzing on-going or past cyber attacks and failures is identified, collected, and preserved in accordance with NNSA and site policies.

n. Intrusion Detection and Response. Measures to detect unauthorized attempts to penetrate the system and respond to detected incidents. This measure supports the Intrusion Detection and Response principle.

P.IDS	The information system is protected from unauthorized attacks or penetrations of the information system.

o. Malicious Code Detection. Measures to protect an information system against software or firmware designed to adversely impact the confidentiality, integrity or availability of the information system. This measure supports the Data Assurance, Entity Integrity, Intrusion Detection and Response, Least Privilege, and Malicious Code principles.

P.MALICIOUS_CODE	The information system is protected from hardware, software, and firmware designed to adversely impact the confidentiality, integrity, and availability of the system and information assets.

p. Marking And Review Of Hardware, Output, And Media. Measures to ensure that the sensitivity of information is unambiguously associated with the written or electronic representation of information. All major components of the information system, output and removable media must be marked in accordance with NNSA policies and site procedures. All media (paper, disks, zip drives, removable hard drives, etc.) must be reviewed for classification and sensitivity and properly marked, in accordance with NNSA policies and site procedures, before release. All electronic communications (e.g., email, email attachments, web-based (HTML, XML, etc.), FTP, etc.)) must be reviewed for classification and sensitivity before release outside the system boundary. This measure supports the Education and Awareness, Marking and Review of Hardware, Output, and Media, and Secure System Management, Control, and Operation principles.

P.FILE_REVIEW	An automated or administrative classification and sensitivity review is performed on all electronic communications and files that are to be electronically transmitted beyond the system boundary before release.
P.MEDIA_MARKING	All removable media components of the information system and output inside the system boundary are

appropriately marked with the level of the highest information sensitivity of information that the system is accredited to operate; or marked in accordance with a classification review or information sensitivity review by authorized personnel.

P.MEDIA_REVIEW — All media (paper, disks, zip drives, removable disk drives, etc.) are reviewed for classification and sensitivity and properly marked before release outside the system boundary.

q. Personnel. Personnel with system access play an integral role in protecting information, defining system security policies, and maintaining and monitoring the confidentiality, integrity, and availability attributes that are inherent within the information systems. Personnel directly involved with a system may be users, operators, administrators, Communications Security (COMSEC) custodians, and developers and maintainers. Duties, responsibilities, privileges, and specific limitations of information systems users, both general and privileged, must be specified in writing. This measure supports the Least Privilege and Personnel Security principles.

P.PERSONNEL — All users (including privileged users) are cleared, or have appropriate background reviews (whichever is appropriate), according to NNSA and DOE policies, for the highest level of information sensitivity, have formal access approval for, and an authorized need-to-know for, the information to which he/she is allowed access.

P.ROLE_SEPARATION — Security roles and responsibilities are distributed to preclude any one individual from adversely affecting operations or the integrity of the system.

P.TRUSTED_USER — All users shall abide by designated policies and the conduct stated by those policies. In this context, 'users' includes both users of systems that interface with the TOE, and the administrators of systems that interface with the TOE in addition to the administrators of the TOE. This policy covers use and adherence to policies, procedures, system, admin, and user documentation, associated with the TOE and all systems that interface with the TOE.

r. Physical. The information and information system resources must be physically protected. The information and information resources that must be physically protected in order to ensure that security objectives are met will be located within controlled access facilities that mitigate unauthorized, physical access. The information and information system resources must be physically protected in

accordance with NNSA and site policies and procedures. This measure supports the Least Privilege and Physical Security principles.

Information must be protected in accordance with DOE 5632.1C-1, *Manual For Protection And Control Of Safeguards And Security Interests*, and DOE O 471.2x, *Information Security Program*.

P.PHYSICAL	The information and information system resources (including media) are physically protected according to the sensitivity of the information processed, stored, or transmitted by the components.

s. Residual Information Protection. Measures must be implemented to ensure that a resource (logical or physical) does not contain residual data prior to the resource being made available to other entities or environments. The information system must ensure that an internal resource contains no residual data before being re-assigned, allocated, or re-allocated to a different user. This measure supports the Access Controls, Physical Security, and Residual Information Protection principles.

Sanitization is the process of removing the data from media (such that data recovery is not possible) before reusing the media in an environment that does not provide an acceptable level of protection for the data that was in the media before sanitizing.

Information system components used to collect, create, process, transmit, store, or disseminate classified information must be sanitized before they are released from classified information control or released for use at a lower classification level.

Clearing, i.e., overwriting at least 3 times with different or random patterns of bits, is the removal of data from a system component or media performed in a manner that will not allow the data to be reconstructed using normal systems capabilities (e.g., through the keyboard, using software utilities, etc.).

Clearing (not sanitization) is required to release components or removable media from unclassified processing environments operating at either the Medium or Low level of consequence. Sanitization or clearing must be accomplished using a DAA approved procedure.

P.RESIDUAL_DATA	All information system resources are cleared before reallocation of the resource to a different user or environment.

t. Risk Assessment. Measures must be implemented to assess the impact of threats to resources by the exploitation of vulnerabilities and to identify cost-effective countermeasures to reduce risks to an acceptable level. Corrective action plans must be developed for those vulnerabilities that are determined to be detrimental

to the systems security program. This measure supports the Risk Assessment principle.

P.RISKASSESS	Identification of system and environment vulnerabilities and an assessment of their impact on the system's security are regularly performed.

u. Secure System Management. Measures must be implemented to ensure the management, control and separation of security critical functions. The level of security afforded the information and information system must be in accordance with what is generally considered adequate within the business or government sectors where the NNSA element is operating. This measure supports the Secure System Management, Control, and Operation principle.

P.DENY_ACCESS	System resources are controlled to ensure access to information sources cannot be denied to authorized users.
P.DUE_CARE	The information and information system resources are implemented and operated in a manner that represents due care and diligence with respect to risks to the information and the organization.
P.INFO_FLOW	Information flow between information system components is controlled in accordance with established information flow policies.
P.PROTCTD_DOMAIN	The information system security functions maintain a separate protected security domain for their own execution. The components necessary for enforcing the security policies of the information system security functions shall maintain a security domain for their own execution that protects them from interference and tampering by other system activities and users.

v. Session Control. Measures, over and above identification and authentication, must be implemented for the establishment of a secure user session. Site policies must address the control of multiple logons and time outs due to user inactivity. But is there any "minimum" set? The system must immediately notify the user during interactive sessions of changes in security levels or compartments. This measure supports the Access Controls, Education and Awareness, Least Privilege, Secure System Management, Control, and Operation, and Session Control principles.

P.SESSION_CTL	User access to a system is determined by the authenticated user's access profile.
P.WARNING_BANNER	All authorized users are notified that they are subject to being monitored, recorded, and audited through the use

of an NNSA approved warning text and positive acknowledgement by the user is required before granting the user access to system resources.

The warning banner must be displayed on the initial screen (before a user is granted any access to system resources) and require user action acknowledging their consent to monitoring and disclosure. If the operating system does not have a routine facility for a system manager or user to insert an initial screen notice (without access to source or esoteric commands) other methods of notification must be developed and documented in the information system Security Plan. At a minimum, these methods must include: 1) Posting of a notice, containing the warning banner text, in a highly visible position on or near the location(s) where users may access the system, and 2) Incorporation of the warning banner text in all agreements signed by the user to obtain information system access. The minimum required warning banner text is:

NOTICE TO USERS

This is a Federal computer system and is the property of the United States Government. It is for authorized use only. **Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.**

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, Department of Energy, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. **By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or Department of Energy personnel.**

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

w. System Assurance. Measures must be implemented to ensure that the security critical components of an information system are able to protect themselves from unauthorized access. This measure supports the Configuration Management, Risk Management, Secure System Management, Control, and Operation, and System Assurance principles.

P.SYS_ASSURANCE The information system's security policy is maintained in the environment of distributed systems even if the systems are interconnected via an insecure networking medium (wire-lines, fiber, Internet, wireless, etc.).

P.SURVIVE	The system in conjunction with its environment must be resilient to insecurity, resisting the insecurity and/ or providing the means to detect an insecurity and recover from it.

x. System Recovery. At a minimum, systems features must be implemented to ensure system recovery is accomplished in a controlled manner. This measure supports the System Recovery and Secure System Management, Control, and Operation principles.

P.SYS_RECOVERY	Controlled or trusted secure system recovery occurs in the event of an information system failure.

y. Testing. Measures must be implemented for exercising and evaluating the operation of the system. This measure supports the Risk Assessment, Secure System Management, Control, and Operation, and Testing principles.

P.SYS_TESTING	Certification and post-accreditation testing is applied to the information system in accordance with PCSP and DAA requirements.

z. User Identification. Measures used to unambiguously link a user's identity to security attributes (e.g., role, clearances, formal access approvals, and need-to-know). Identification and authentication are required to ensure that users are associated with the proper security attributes, such as identity or location. This measure supports the Access Controls, Audit, Authentication, Data Assurance, Least Privilege, and User Identification principles.

P.UNIQUE_ID	Every authenticated user of an information system is uniquely identified.

aa. Waste, Fraud, and Abuse Protection. Waste Fraud and Abuse must be detected or prevented and reported in accordance with NNSA policies and site procedures. This measure supports the Secure System Management, Control, and Operation and Waste, Fraud, and Abuse Protection principles.

P.WFA	Waste Fraud and Abuse is detected or prevented and reported in accordance with DOE O 221.1, *Reporting Waste Fraud, and Abuse to the Office of IG*.

This page intentionally blank.

CHAPTER VI

INFORMATION SYSTEM CERTIFICATION AND ACCREDITATION PROCESS

1. IINTRODUCTION. The NNSA Information Security Certification and Accreditation Process (ISCAP) establishes a standard NNSA approach to ensure a system is accredited to operate in a specified computing environment with an acceptable level of risk throughout its life cycle. The ISCAP activities standardize the C&A process to support a risk management focus on the mission, environment, and architecture for NNSA information systems.

2. Life Cycle and Tailoring. The ISCAP applies throughout the life of all NNSA information systems. It is adaptable to any type of information technology system, any computing environment, and mission. It may be adapted to include existing system certifications, evaluated products, new security technology or programs, and adjust to applicable standards. The ISCAP may be mapped to any system life-cycle process. The activities defined in the four ISCAP phases are mandatory. However, implementation details of these activities may be tailored, and where applicable, integrated with other activities and documentation.

3. Roles and Responsibilities. C&A is generally accomplished by a minimum of three individuals: the System Owner, the DAA, and the CSSM. Additional roles may be added to increase the integrity and objectivity of C&A decisions in support of the system business case or mission. For example, the CSSO, who may represent the system owner, usually performs a key role in the maintenance of the security posture after the accreditation and may also play a key role in the C&A of the system. The ISCAP allows these individuals to tailor and scope the C&A efforts to the particular mission, environment, system architecture, threats, funding, and schedule of the system.

   NOTE: The following sections provide an overview of the ISCAP roles and responsibilities. Responsibilities of the primary C&A roles in each life cycle phase are shown in Table 5.

Table 5. Certification and Accreditation Roles

	System Owner (May be represented by the CSSO)	DAA	CSSM
Phase 1	• Initiate security dialogue with DAA and CSSM • Define system schedule and budget • Support ISCAP tailoring and level of effort determination • Define system architecture • Prepare life cycle management plans • Define security architecture • Draft or support drafting the Security Plan, PP, ST[1]	• Define accreditation requirements • Obtain threat assessment • Assures the CSSM is assigned • Support ISCAP tailoring • Approve the Security Plan • Approve Security Targets	• Begin Vulnerability and risk assessments • Review threat definition • Lead ISCAP tailoring • Determine level of certification effort • Describe certification team roles and responsibilities • Support drafting the Security Plan[1]
Phase 2	• Develop system or system modifications • Support certification activities • Review certification results • Revise system as needed • Resolve security discrepancies	• Support certification activities	• Conduct certification activities • Assess vulnerabilities • Report result to the System Owner, and DAA • Determine if system is ready for certification
Phase 3	• Support certification activities • Provide access for security test and evaluation • Provide system corrections	• Assess vulnerabilities and residual risk • Decide to accredit, grant an interim approval to operate (IATO), or terminate system operations	• Conduct certification activities • Evaluate security requirements compliance • Assess vulnerabilities and residual risk • Report results of assessments to the System Owner and DAA • Recommend risk mitigation measures • Prepare C&A accreditation package • Recommend system accreditation
Phase 4	• Update information system to address Phase 3 reported vulnerabilities and patches under configuration management • Report information system security related changes to the DAA and CSSM • Review and update life cycle management policies and standards[1] • Resolve security discrepancies • Comply with Security Plan	• Review the Security Plan • Review proposed changes • Oversee compliance validation • Decide to accredit, IATO, or, if SSP is no longer valid, terminate system operations	• Ensure and assess system security throughout it's lifecycle

[1] The information system Cyber System Security Officers (CSSO) may be requested to develop these documents.

4. REQUIREMENTS.

   a. Each information system must be accredited every 3 years or when security significant changes have been made in the information system.

   b. Each information system must receive an "accreditation" or an "interim approval to operate" (IATO) before beginning operational activities.

   c. Each information system must be included in a Security Plan.

   d. The SSP must be used as the basis for all certification, accreditation, and security operation activities.

   e. A SSP must include the items identified in Attachment 4.

   f. The DAA must ensure the completion of all activities defined for the ISCAP.

   g. The scope and level of effort for certification of an information system must be based on the highest Consequence of Loss of confidentiality, integrity, and availability for all information groups on the information system as shown in Table 6.

Table 6. Certification Levels

Consequence of Loss of Confidentiality	Certification Level	Description
Very Low	Level 1	Scope and content of certification negotiated between cognizant DAA, CSSM, and System Owner.
Low	Level 2	Scope and content of certification negotiated between cognizant DAA, CSSM, and System Owner with testing of all security functionality and verification of assurance components.
Medium	Level 3	Scope and content of certification established by the cognizant DAA with security functionality structurally analyzed and verification of assurance components.
High	Level 4	Minimum Analysis - Requires completion of an approved Security Test and Evaluation Plan that provides for methodical test and evaluation of all security functionality and verification of assurance components.
Very High	Level 5	Detailed Analysis - Requires completion of an approved Security Test and Evaluation Plan that provides for methodical test and evaluation of all security functionality and verification of assurance components. Requires an in-depth, independent design review and analysis of security functionality (e.g., verification and validation) defined by the DAA.

5. SYSTEM SECURITY PLAN. The principal document in the ISCAP is the System Security Plan. The SSP documents the security environment in which the information system exists; the cyber security requirements needed to protect the information on the system, and the conditions for C&A of the information system. The SSP is a formal agreement among the System Owner, CSSM, and DAA. The SSP is used throughout the entire system lifecycle and ISCAP process to guide actions, document

decisions, specify cyber security requirements, document solutions, and define the system's security configuration throughout its life.

a. SECURITY PLAN. The structure of the SSP depends on the certification complexity and organizational requirements. The SSP is intended to consolidate security-related documentation into one document. Attachment 4 contains a sample SSP format.

(1) Coverage. Each information system must have a Security Plan. In some cases, a single SSP may include several systems. For example, in Site or Type accreditations, a SSP may be prepared for the system (software and hardware) and implemented in a similar environment at each location where the software and hardware will be employed.

(2) SSP Tailoring. The DAA, CSSM, and System Owner, have the authority to tailor the SSP to meet operational requirements, security policy, and prudent risk management. The SSP must be flexible enough to permit adjustment throughout the system's life cycle as conditions warrant. New requirements may emerge from design necessities, existing requirements may need to be modified, or the DAA's view of acceptable risk may change. In such a case, the SSP is updated to accommodate the requirements. The SSP is developed in the Definition phase and updated in each phase as the system develops and new information becomes available. When feasible, the SSP can be tailored to incorporate other documents as appendices or by reference. The completed SSP must contain those items required by the DAA.

(3) SSP Contents. The minimum information that must be in a SSP is listed in Attachment 4.

a. Forms Of Accreditation. Three forms of accreditation are possible:

(1) System Accreditation. This is an information system (general support system, major application, stand-alone, etc.) that is operating under a single Security Plan. Accreditation is based on the system certification. Note: This includes controlled interfaces or other systems that interface with off site non-NNSA systems.

(2) Site Accreditation. A Site accreditation is a master plan approach and evaluates the applications and information systems at a site or specific location(s) within a site operating in a similar environment and under one set of rules. The information systems are operating under a single Security Plan. All information systems under the SSP are contained within the Site or under the cognizance of the Computer Security Site Manager. Accreditation is based on the certification of the first system and the follow-on certification process for certifying additional information systems. The authority to operate additional systems under the SSP is based on successful completion of the C&A process described in the Security Plan.

(3) Type Accreditation. A Type accreditation evaluates a major application or information system that is distributed among different sites and operating in similar environments and under one set of rules. This is a master plan approach where the accreditation extends across Site boundaries. The enterprise systems (general support system, major application, stand alone, etc.) involved may or may not be interconnected. However, the major application or information system is operating under a single Security Plan, such as SecureNet and the NNSA Office of Secure Transportation's Transportation Command and Control System. Accreditation to operate an implementation of the application or system at a site is based on the C&A process described in the Security Plan.

b. Interim Approval To Operate. An "Interim Approval to Operate" may be granted if the system does not meet the requirements as stated in the Security Plan, but operational need may mandate that the system become operational. The IATO is a temporary approval that may be issued for no more than a maximum of 180 days. The initial IATO may not be renewed.

6. CERTIFICATION AND ACCREDITATION PHASES. The ISCAP is composed of four phases: Definition, Verification, Validation, and Post Accreditation. Throughout this section, ISCAP activities are listed for each phase that identifies the type of activity that should be accomplished in that phase.

a. Definition. This phase is focused on understanding the information system business case, environment, and architecture to determine the security requirements and activities necessary to achieve C&A. The objective of this phase is to agree on and document the security requirements, C&A perimeter, schedule, and resources required to complete the C&A. The specific C&A activities and the levels of effort associated with each of the activities depend on environment, threat and other considerations. The certification plan developed in the Definition phase must reflect this fact. Activities in this phase, based on the Certification Level, may include:

- Prepare the Mission Description and System Identification
- Notify the DAA and CSSM (Register the System)
- Prepare the Environment and Threat Description
- Determine the Information Groups
- Prepare the System Architecture Description
- Determine the Information System PP(s) or ST(s)
- Determine the System Security Requirements
- Tailor the SSP contents
- Determine Certification Level
- Draft the Security Plan

b. Verification. This phase verifies the system's compliance with the information in the Security Plan. The objective of this phase is to ensure the fully integrated system will be ready for certification testing. Activities in this phase, based on the Certification Level, may include:

- System Architecture Analysis
- Software Design Analysis
- Network Connection Rule Compliance Analysis
- Integrity Analysis of Integrated Products
- Life-Cycle Management Analysis
- Vulnerability Assessment

c. Validation. This phase validates compliance of the fully integrated system with the security requirements as stated in the Security Plan. The objective of this phase is to produce the required evidence to support the DAA in making an informed decision to grant accreditation to operate the system. Activities in this phase, based on the Certification Level, may include:

- System Test and Evaluation (ST&E)
- Penetration Testing
- Validate Protected Transmission System compliance
- System Management Analysis
- Contingency Plan Evaluation
- Risk Management Review

c. Post Accreditation. This phase starts after the information system has been certified and accredited. This phase includes those activities necessary for the continued operation of the information system in its computing environment and to address the changing threats and small-scale changes a system faces throughout its life cycle. The objective of this phase is to ensure secure system management, operation, and maintenance to preserve an acceptable level of residual risk. Activities in this phase, based on the Certification Level, may include:

- SSP Maintenance
- Physical, Personnel and Management Control Review
- Contingency Plan Testing
- Maintain TEMPEST Compliance
- Maintain PTS Compliance
- Change Management
- Risk Management

This page intentionally blank.

CHAPTER VII

DEVIATIONS FROM THE NNSA CYBER SECURITY PROGRAM

1. INTRODUCTION. This chapter describes the types of deviations (variances, waivers, and exceptions), required justification, and process for obtaining deviations from the NNSA PCSP requirements.

2. REQUIREMENTS. All approved deviations, as described below, must be documented in the System Security Plan for the information system or the Site Safeguards and Security Plan or Site Security Plan, as appropriate.

   a. Variances. Variances are approved conditions that technically vary from a NNSA PCSP requirement, but afford equivalent levels of protection without compensatory measures.

      (1) Variance requests must be submitted in writing through the cognizant CSOM to the cognizant DAA. The variance request must include detailed description of the requirement and rationale for the variance. The variance documentation must be included, or referenced, in the information system Security Plan.

      (2) The cognizant DAA will review and approve, in writing, or disapprove with comments and recommendations.

      (3) Variances may be approved for up to three years, but must be submitted for reconsideration whenever the information system is accredited or re-accredited.

   b. Waivers. Waivers are approved non-standard conditions that deviate from a NNSA PCSP requirement, which, if uncompensated, would create a potential or real cyber security vulnerability. Waivers require implementation of compensatory measures that will be in effect for the duration of the waiver.

      (1) Waiver requests and supporting documentation must be submitted in writing through the cognizant CSOM to the cognizant DAA for review.

      (2) Documentation supporting the waiver request must identify the requirement(s) to be waived, indicate the compensatory measures implemented, and, if appropriate, that performance testing has been completed to validate the compensatory measures.

      (3) The DAA will forward the waiver request, and documented recommendation for approval, to the NNSA CSPM.

      (4) The NNSA CSPM will approve or disapprove the waiver request and provide a final decision in writing to the cognizant DAA.

(5) The cognizant DAA will notify the cognizant CSOM who will notify the site CSSM and the information system CSSO.

(6) Approved waivers may remain in effect for up to two years and must be documented in the information system Security Plan. If an extension is necessary, the waiver request must be re-submitted.

c. Exceptions. Exceptions are approved deviations from an NNSA PCSP requirement that creates a security vulnerability. Exceptions shall only be approved when correction of the condition is not feasible or cost effective and compensatory measures are inadequate to preclude the acceptance of risk.

(1) Requests for exceptions and supporting documentation must be submitted in writing through the cognizant CSOM to the cognizant DAA for review.

(2) Documentation supporting the exception request must identify the requirement(s) that cannot be met, indicate the compensatory measures implemented, and, if appropriate, that performance testing has been completed to validate the compensatory measures.

(3) The DAA will forward the exception request, and documented recommendation for approval, to the NNSA CSPM.

(4) The NNSA CSPM will approve or disapprove the exception request and provide a final decision in writing to the cognizant DAA.

(5) The cognizant DAA will notify the cognizant CSOM who will notify the site CSSM and the information system CSSO.

(6) Approved exceptions may remain in effect for one year.

(7) The cognizant DAA must review and validate the need for each exception.

(8) Exceptions must be documented in the information system Security Plan.

CHAPTER VIII

CYBER SECURITY PROGRAM PLAN

1. INTRODUCTION. The NNSA element Cyber Security Program Plan (CSPP) is the document which outlines the policies, procedures and practices of an organization's, (e.g. an NNSA element) cyber security program – classified and unclassified. The CSPP is a top-level, stand-alone program document at the management level and details the organization's policies, procedures and practices for ensuring effective cyber security. It also explains the organization's specific environment, missions and threats. The CSPP should be integrated with other program plans in the organization (e.g., Site Safeguards and Security Plan (SSSP), Information Resource Management (IRM) plans, etc.).

2. CSPP CONTENTS. The CSPP must describe how the organization implements the NNSA PCSP. The CSPP must explain the organization's specific environment, missions, and threats, and describe the policies, procedures and practices for ensuring effective cyber security. If the following requirements can be met with existing organization policies or procedures the policy/ procedures should be summarized and referenced in the CSPP and a copy of the organization policy or procedure attached to the CSPP.

   a. Environment. Describe the mission and objectives, and security environment for the element.

   b. Information Groups. Identify the Information Groups (see Attachment 3 for a description of the Information Groups) handled by the element.

   c. Element Unique Threats. Reference or document any threat/ threat assessments (e.g., NNSA Threat Assessment, OPSEC Threat Assessments, Site Unique Threats, etc.) used as the basis for its threat environment

   d. Roles and Responsibilities. Define the element cyber security, CSSM, CSSO, System Administrator, user, etc. roles and responsibilities for the element.

   e. Program/Project Controls And Accountability. Describe the method for tracking the element's implementation of the NNSA PCSP in terms of cost and schedule.

   f. Information Systems. Reference an inventory of information systems (accredited and in the accreditation process).

   g. C&A Program. Describe the element's information system C&A process.

h. Security Significant Changes. Define changes to information system components that will be considered 'security significant.'

i. Equipment Management.

(1) Configuration Management. Describe the element's configuration management policies and procedures.

(2) Equipment Maintenance. Describe the maintenance policies and procedures; including the introduction of vendor maintenance hardware, software, and firmware and the management of remote maintenance activities.

(3) Clearing and Sanitization. Describe the procedures for clearing and sanitization of information system components.

(4) Decommissioning. Describe the procedures for decommissioning information systems.

j. Incident Warning And Advisory Responses. Describe the incident warning and advisory response process for the element. Describe the composition of the element incident response team and the contact methods (numbers for telephones, pages, cell phones, e-mail, etc.).

k. INFOrmation CONdition (INFOCON). Describe the process for establishing, changing, and reporting the element's INFOCON status. Describe the element's response measures for each INFOCON level.

l. Security Monitoring. Describe the element's security monitoring policy, processes and procedures, including how monitoring is used to mitigate risks to the element. Describe the element's process, and procedures for detecting and managing intrusion detection at the desktop, network, and element levels.

m. Security Coordination. Describe the element's process and procedures to ensure coordination with other security programs, such as physical security, personnel security, TSCM, TEMPEST, CMPC, PTS, OPSEC, and COMSEC.

n. Malicious Code. Describe the element process and procedures to address malicious code (e.g., handled at boundary, handled at desktops, and handled at selected locations), the mechanisms employed, and frequency of updating anti-malicious code software throughout the element.

o. Denial of Service / Continuity of Service. Describe the process for identifying those information systems and networks that, due to mission operation necessities, have a low tolerance for disruption or unavailability and the procedures and mechanisms that will be employed to limit and recover from such disruption or unavailability.

p. Internet Security: Describe the element's Internet use policy, method of securing the element's network from external threats via the Internet connection, policies and procedures for reviews of web page and server content, web page and server monitoring policy.

q. Email: Describe the element's email policy, including controls for the use of off-site email.

r. Component and Output Marking and Labeling: Describe the element's policy for marking and labeling the sensitivity or classification levels of computers, computer equipment, media storage devices, and computer output.

s. Clear Text Password Management. Describe the element's program for the elimination of clear text passwords from existing and future information systems.

t. Data backup and restoration. Describe the element's policies for data backup and restoration.

u. Disaster Recovery Program. Describe the element's disaster recovery program, including the policies and procedures for regular testing of continuity of service plans.

v. Output and Display Device Access. Describe the element's policies for controlling access to system output and display devices.

w. Hardware and Software Technical Reviews. Describe the process for performing technical reviews of the hardware and software components of portable computers that are taken or used outside the United States or may have been under the control of a non-U.S. government organization.

x. Portable Computing Devices. Describe the policies and procedures for managing the use of portable computing devices, including personal electronic devices, in all areas of the element.

y. Wireless Information Systems. Describes the policies and procedures for managing the installation and use of radio frequency (RF) systems in all areas of the element.

z. Risk Management. Describe the element's process for risk management for all information systems and information system components.

aa. Training. Describe the process for cyber security training; including who must receive training and how frequently re-training will occur. Describe the methodology being used for training (e.g., briefings, email), identify those positions requiring training, and identify (by title/position) those responsible for overseeing training activities at the element.

bb. Performance Assessment. Describe the element's process and metrics employed to assess compliance with the CSPP and the process for evolving these metrics. Describe the element's peer review and self assessment processes including, the frequency of reviews, the process for selecting peer review members, qualifications required of the prospective individuals or entities, and who is responsible for selecting peer review participants.

cc. Plan Change Management. Describe the update frequency for the CSPP and the process for updating the plan.

ATTACHMENT 1

ACRONYMS AND ABBREVIATIONS

AA	Approving Authority
C&A	Certification and Accreditation
COMSEC	Communication Security
COTS	Commercial Off-The-Shelf
CSSM	Cyber Security Site Manager
CSSO	Cyber System Security Officer
CSOM	Cyber Security Office Manager
DAA	Designated Approving Authority
FISCAM	Federal Information Systems Controls Audit Manual
GOTS	Government Off-The-Shelf
IATO	Interim Approval to Operate
NIACAP	National Information Assurance Certification and Accreditation Process
NIST	National Institute of Standards and Technology
NISPOM	National Industrial Security Program Operating Manual
NSA	National Security Agency
NSI	National Security Information
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSTISSP	National Security Telecommunications and Information Systems Security Policy
OMB	Office of Management and Budget
OPSEC	Operations Security

PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SP	Special Publication
ST	Security Target
TEMPEST	not an acronym
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy

ATTACHMENT 2

DEFINITIONS

The following are terms and definitions used in this NAP that are not found in National Security Telecommunications and Information Systems Security (NSTISSC) 4009, National Information Systems Security (INFOSEC) Glossary, dated 5 June 1992. "

Accreditation	Formal declaration by the DAA that an information system is accredited to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Architecture	The configuration of any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment and services, including support services and related resources.
Assurance	Measure of confidence that the security features, practices, procedures and architecture of an information system accurately mediate and enforce the security policy.
Boundary	The conceptual limit of an information system that extends to all directly and indirectly connected users who receive output from the system without a reliable human review by an appropriately authorized or cleared authority.
Certification	Comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements.
Certification and Accreditation (C&A) perimeter (See Perimeter below)	
	All components of a system that are to be accredited by the DAA and excluding separately accredited systems to which the system is connected.

Communications Security (COMSEC)

Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes crypto security, transmission security, emission security, and physical security of COMSEC material.

Computing Environment — The total environment in which an automated information system, network, or a component operates. The environment includes physical, administrative, and personnel procedures as well as a communication and networking relationship with other information systems.

Confidentiality — A security objective that seeks to assure that information is not disclosed to unauthorized persons, processes, or devices. (NSTISSI No. 4009: Assurance that information is not disclosed to unauthorized persons, processes, or devices.)

Consequence of Loss — An expression of the consequences of loss of the information's integrity, availability, or confidentiality.

Cyber Security Site Manager (CSSM)

a. The official responsible for performing the comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meet a set of specified security requirements, and ensuring the approved security configuration is maintained.

b. The individual responsible for implementing a cyber security program at a site.

Cyber System Security Officer (CSSO)

Person responsible to the system owner and designated approving authority for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with system security officer.

Data Integrity	Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
Data Owner	The person responsible for having information reviewed for sensitivity and classification. This person is responsible for its generation, management, and destruction.
Data Steward	The person acting on behalf of the data owner for the generation, management, and destruction of data and to ensure the review of information sensitivity and classification.
Designated Approving Authority (DAA)	Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority.
Direct User	A user with physical or electronic access to any component of the information system.
Environment	Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system.
Formal Access Approval	Access to information is authorized in writing with justification. Documented approval by a data owner or data steward to allow access to information. For example, formal assignment to process personnel or health records is documented evidence of formal access approval to unclassified Privacy Act information, and formal assignment to process budget or contract information is documented evidence of formal access approval to Unclassified Protected Information.
General Support System	An interconnected set of information resources under the same direct management control that share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide

	backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. [From Office of Management and Budget (OMB) Circular A-130, Appendix III.]
Information integrity	The preservation of unaltered states as information is transferred through the system and between components.
Information System	The infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. Any telecommunication or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware. [Office of Management and Budget, Circular A-130, Nov 30, 2000: A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.]
Information technology (IT)	The hardware, firmware, and software used as part of the information system to perform information functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (1) requires the use of such equipment, or

	(2) requires the use, to significant extent of such equipment, in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "information technology" does not include national security systems as defined in the Clinger-Cohen Act of 1996 (40 U.S.C. 1452). [Office of Management and Budget, Circular A-130, Nov 30, 2000.]
Information System Certification and Accreditation Process (ISCAP)	
	The standard NNSA process for identifying information security requirements, providing security solutions, managing information system security activities, and authorizing the operation of a system.
Integrity	Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. It is composed of data integrity and system integrity
Interim approval to operate (IATO)	
	The system does not meet the requirements as stated in the System Security plan, but mission criticality mandates the system become operational. The IATO is a temporary approval that may be issued for no more than a six-month period.
Legacy information system	An operational information system that existed prior to the implementation of the C&A process.
Major Application	A major application is an application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them,

	however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. [From Appendix III, OMB A-130] An application that requires special management attention because of its importance to an organizations' mission; its high development, operating, or maintenance costs; or its significant role in the administration of an organization's programs, finances, property, or other resources. Site management determines organizational scope and the definition of "significant" role.
Mission	The assigned duties to be performed by an information system.
Perimeter	All components of an information system that are to be accredited as one entity.
Personally Owned	An item that is owned by an individual and is intended solely for his/her personal use.
Portable Computing Device	Portable Computing Devices are any portable devices that provide the capability to collect, create, process, transmit, store, and disseminate information. They include (but are not limited to) Personal Digital Assistants (PDAs), palm tops, hand-held or portable computers and workstations, non-web-enabled cell phones, web based enhanced cell phones, two-way pagers, and wireless e-mail devices.
Privileged User	A user with access to control, monitoring, or administration functions of the information system (e.g., system administrator, system security officer, maintainers, system programmers, etc.). NOTE: It is often convenient to refer to a user who is NOT a privileged user as a general user.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of information systems that meet specific protection measures for specific information groups.
Risk assessment	Process of analyzing threats to and vulnerabilities of an information system and the potential impact the loss of

	information or capabilities of a system would have on national security. The resulting analysis is a basis for identifying appropriate and cost-effective countermeasures.
Risk management	The process concerned with the identification, measurement, control, and minimization of security risks in information systems to a level commensurate with the value of the assets protected.
Security	Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.
Security Documentation	All documents which describe the security requirements, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system or major application (or update to either) meets the protection requirements.
Security Function (SF)	Part or parts of the information system that have to be relied upon for enforcing a closely related subset of the rules from the TSP.
Security Function Policy (SFP)	The security policy enforced by an SF.
Security Process	The series of activities that monitor, evaluate, test, certify, accredit, and maintain the system accreditation throughout the system life cycle.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation (certification) of an information system.
Site	An NNSA facility: can be a NNSA Service Center, NNSA Site Office, NNSA contractor or subcontractor facility, or the NNSA Headquarters activity that has a responsibility to protect NNSA information systems. It has a set of geographical boundaries as defined in a NNSA SSSP or SSP.
Site Manager	The person responsible for management of all activities at an element.
System	The set of interrelated components consisting of mission, environment, and architecture as a whole.

System Owner	The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system. The system owner, based on previous information, also has some security duties.
Security Plan	A formal agreement among the DAA, the CSSM(s), and the System Owner(s). It is used throughout the ISCAP to guide actions, and to document decisions, security requirements, certification tailoring and level-of-effort, certification results, CSSM's certification, and the DAA's accreditation to operate.
Target of Evaluation (TOE)	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected and distributed within a TOE.
User	An individual who can receive information from, input information to, or modify information on an information system without an independent human review. In a processing context, this also includes a process acting on behalf of a user.
Vulnerability assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

ATTACHMENT 3

1. Information Groups. An information group contains all information that requires similar protection or is similar in content or use. The following information groups have been defined for use in assessing the cyber threats to information and for use in defining the minimum protection requirements for each information group. The information groups and sub-groups are:

   a. **Open, Public, Unrestricted** -- Information that requires no protection from disclosure, e.g. approved for public release.

   b. **Unclassified Protected** -- Information designated as requiring protection by the data owner or data steward.

   c. **Unclassified Mandatory Protection** -- Unclassified information requiring protection mandated by policy, laws, such as

      - Privacy Act information;
      - Agreements between Department of Energy (DOE), NNSA, its contractors, and other entities such as commercial organizations or foreign governments;
      - Proprietary information (but not third party proprietary);
      - Unclassified Controlled Nuclear Information (UCNI);
      - Export-controlled information (ECI);
      - Naval Nuclear Propulsion Information (NNPI);
      - Military/ dual use information (such as the Critical Military Technology and Materials list identified by DoD);
      - Nonproliferation information; and
      - Information exempt from the Freedom of Information Act (FOIA), FOIA exemptions are:
        - **Exemption One** : Records which are specifically authorized under criteria established by an Executive Order to be kept secret in interest of national defense or foreign policy and are in fact properly classified pursuant to such Executive Order;
        - **Exemption Two** : Records related solely to the internal personnel rules and practices of the FDIC;
        - **Exemption Three**: Records specifically exempted from disclosure by statute, provided that such statute:

          a. Requires that the matters be withheld from the public in such a manner as to leave no discretion on the issues; or

b. Establishes particular criteria for withholding or refers to particular types of matters to be withheld.

- **Exemption Four**: Trade secrets and commercial or financial information obtained from a person that is privileged or confidential;
- **Exemption Five**: Interagency or intra-agency memoranda or letters which would not be available by law to a private party in litigation with the FDIC;
- **Exemption Six**: Personnel, medical, and similar files (including financial files) the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- **Exemption Seven**: Records compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records:
  - Could reasonably be expected to interfere with enforcement proceedings;
  - Would deprive a person of a right to a fair trial or an impartial adjudication;
  - Could reasonably be expected to constitute an unwarranted invasion of personal privacy;
  - Could reasonably be expected to disclose the identity of a confidential source, including a state, local, or foreign agency or authority or any private institution that furnished records on a confidential basis;
  - Would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law; or
  - Could reasonably be expected to endanger the life or physical safety of any individual.
- **Exemption Eight**: Records that are contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of the FDIC or any agency responsible for the regulation or supervision of financial institutions; and
- **Exemption Nine**: Geological and geophysical information and data, including maps, concerning wells.

d. **Confidential Non-Nuclear Weapons** -- Information that is classified Confidential National Security Information, Confidential Formerly Restricted Data, Secret National Security Information, or Secret Formerly Restricted Data

and does not contain any nuclear weapons data but may contain information related to uranium enrichment.

e. **Secret Non-Nuclear Weapons Data** -- Information that is classified Secret Restricted Data and does not contain any nuclear weapons data; but may contain information related to uranium enrichment or other Secret Restricted Data.

f. **Confidential Restricted Data Sigmas 1 through 13 --** Information that is classified as Confidential and identified as Restricted Data or is related to nuclear weapons. This information is further marked with at least one of the sigma categories 1 through 13.

- **Sigmas 1 and 2**. Theory of operation or complete design of hydrodynamic, nuclear, fission weapons or their unique components. This includes the high explosive system with its detonators and firing unit, pit system, and nuclear initiation system as they pertain to weapon design and theory.
- **Sigmas 3, 4, 5, 6, 7, 8, 9, 10,11, 12, and 13**. Manufacturing and utilization information not comprehensively revealing the theory of operation or design of the physics package; Information inherent in pre-shot and post-shot activities necessary in the testing of atomic weapons or devices; Production rate and/or stockpile quantities of nuclear weapons and their components; General studies not directly related to the design or performance of specific weapons or weapons systems, e.g., reliability studies, fuzing studies, damage studies, aerodynamic studies, etc.; Chemistry metallurgy, and processing of materials peculiar to the field of atomic weapons or nuclear explosive devices; Information concerning inertial confinement fusion that reveals or is indicative of weapon data; Theory of operation or complete design of the nuclear energy converter, energy director, or other nuclear directed energy weapon outside the radiation case of the nuclear source but within the envelope of the nuclear directed energy weapon concept; and Manufacturing and utilization information for nuclear energy converters, directors, or other nuclear directed energy weapon outside the nuclear source radiation case, not comprehensively revealing the theory of operation or design of the nuclear directed energy weapon concept.

g. **Secret Restricted Data Sigmas 1 through 13 --** Information that is classified as Secret and identified as Restricted Data and is related to nuclear weapons. This information is further marked with at least one of the sigma categories 1 through 13.

- **Sigmas 1 and 2**. Theory of operation or complete design of hydrodynamic, nuclear, fission weapons or their unique components. This includes the high explosive system with its detonators and firing unit, pit system, and nuclear initiation system as they pertain to weapon design and theory.
- **Sigmas 3, 4, 5, 6, 7, 8, 9, 10,11, 12, and 13**. Manufacturing and utilization information not comprehensively revealing the theory of operation or design

of the physics package; Information inherent in pre-shot and post-shot activities necessary in the testing of atomic weapons or devices; Production rate and/or stockpile quantities of nuclear weapons and their components; General studies not directly related to the design or performance of specific weapons or weapons systems, e.g., reliability studies, fuzing studies, damage studies, aerodynamic studies, etc.; Chemistry metallurgy, and processing of materials peculiar to the field of atomic weapons or nuclear explosive devices; Information concerning inertial confinement fusion that reveals or is indicative of weapon data; Theory of operation or complete design of the nuclear energy converter, energy director, or other nuclear directed energy weapon outside the radiation case of the nuclear source but within the envelope of the nuclear directed energy weapon concept; and Manufacturing and utilization information for nuclear energy converters, directors, or other nuclear directed energy weapon outside the nuclear source radiation case, not comprehensively revealing the theory of operation or design of the nuclear directed energy weapon concept.

h. **Secret Restricted Data Sigma 14 and 15 -** Information that is classified as Secret and identified as Restricted Data or is related to nuclear weapons. This information is further marked with the sigma category 14 or sigma category 15.

- **Sigma 14**. The category of sensitive information concerning the vulnerability of nuclear weapons to deliberate unauthorized nuclear detonation.
- **Sigma 15**. The category of sensitive information concerning the design and function of nuclear weapons use control systems, features, and their components. This includes use control information for passive and active systems.

i. **Top Secret** -- Information that is classified Top Secret.

j. **Top Secret Restricted Data** -- Nuclear Weapon information that is classified Top Secret.

k. **Special Information Groups** -- These information groups contain confidential or secret restricted data (or other national security data) that the US Government, DOE, or NNSA have determined that special or additional protection is necessary. Examples of this type of information include certain use control, vulnerability, or design data considered the 'crown jewels' or critical to the nuclear weapons program.

ATTACHMENT 4

SECURITY PLAN OUTLINE

1. INTRODUCTION. The SSP is a living document that represents the formal agreement among the DAA, the CSSM, and the System Owner. The SSP is developed in the Definition phase and updated in each phase as the system development progresses and new information becomes available. At minimum, the SSP must contain the following information.

   If the required information is documented in site policies or procedures, the SSP should include only a complete reference to the information.

   1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION
      - 1.1 System Name and Identification
      - 1.2 High Level Description of System
      - 1.3 Functional Description
        - 1.3.1 System Criticality
        - 1.3.2 Information Groups on the information system
        - 1.3.3 Consequence of loss of confidentiality, integrity, and availability for each information group
        - 1.3.4 System User Description and Clearance Level
        - 1.3.5 Need-to-Know requirements
      - 1.4 System Concept of Operations summary
   2. ENVIRONMENT DESCRIPTION
      - 2.1 Operating environment
      - 2.2 Threat Description
      - 2.3 Variances, Waivers, and Exceptions
      - 2.4 Network Connection Rules
   3. SYSTEM ARCHITECTURE DESCRIPTION
      - 3.1 System Description
      - 3.2 System Interfaces and External Connections
      - 3.3 Accreditation Boundary
   4. SYSTEM SECURITY REQUIREMENTS
      - 4.1 Security Target(s)
      - 4.2 Data Security Requirements (expanded/increased requirements by data owner or data steward)
   5. TRAINING

Appendices should be added to include system C&A documents; optional appendices may be added to meet specific needs. All documentation relevant to the systems' C&A should be referenced or included in the Security Plan.

APPENDIX A. Definitions

APPENDIX B. Security Target(s)

APPENDIX C. Security Test and Evaluation Plan and Procedures

APPENDIX D. Certification Statement

APPENDIX E. Risk Assessment Results

APPENDIX F. Approved Variances, Waivers, and Exceptions

APPENDIX G. CSOM Accreditation Recommendation

APPENDIX H. Contingency Plan(s)

APPENDIX I. Memorandums of Agreement – System Interconnect Agreements

APPENDIX J. Accreditation Documentation and Statement

2. SECURITY PLAN DETAILED DESCRIPTION. Each section of the required SSP is briefly described below. The headings for each section match the SSP outline.

1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION

This section describes the system and the mission that the system supports. This includes the name of the organization, the system's name and a stipulation of the system criticality. The mission description is a concise, high-level system specification and needs statement. It describes whom the system will serve, how it will work, what information it will process, how important it is, and why it is being developed. The mission description should come from the mission need document (e.g., Mission Need Statement, Mission Impact Statement, Operational Requirements Document, the purpose statement of the using organization).

1.1 System Name and Identification

This section identifies the system that is being developed or entering the C&A process. This section provides the name and organization of the element developing the mission need and the organizations containing the ultimate user.

1.2 Description of System

The system description provides a complete high-level description of the system architecture. Diagrams or drawings, such as a block diagram, should be included to amplify the description. All components of the system should be described. Identify and describe the physical environment in which the information system will operate including floor plans, equipment placement.

1.3 Functional Description

This section provides a functional description of the system. Include functional diagrams of the system. Describe functions performed jointly with other systems and identify the other systems. Include high-level functional diagrams. Provide the intended flows of data into the system, data manipulation, and product output. For example, a system is required for a local area network (LAN) within an office environment to permit the access of all LAN stations to LAN server resources. In addition, connectivity is required to a wide area network (WAN) for interactive sessions with all other resources having access to the WAN.

1.3.1 System Criticality

This section examines the consequences of a loss of the system. It assesses the effect on element operations or other organizations if they were denied the reliable use of this system. From this analysis, a determination of the system's criticality is made.

1.3.2 Information Groups

This section identifies all information groups to be collected, created, processed, stored, or disseminated on the system

1.3.3 Consequence of loss of confidentiality, integrity, and availability for all information in each information group

This section should state the consequence of loss of confidentiality, integrity and availability for each information group to be collected, created, processed, stored, or disseminated on the system

1.3.4 System User Description and Clearance Levels

This section describes the security clearances of the users

1.3.5 Need-to-Know Requirements

This section describes the need-to-know requirements established by data owner / data steward for each information group on the system.

1.4 System Concept of Operations summary

This information supplements the system description and function statements. A high level description of the concept for the system to satisfy the mission need. Provide a description of those functions that are jointly performed with other systems, and identify the other systems.

2. ENVIRONMENT DESCRIPTION

The environment description documents the intended operational environment, software development and maintenance environment, threat

environment, and external electronic connections. If more than one location is used, provide details of each as a separately numbered heading.

2.1 Operating environment

Describe the access control procedures provided by the environment and any other standard operating procedures that support a secure environment. Provide a description of existing environmental security features that will mitigate the implementation of specific security requirements in that environment rather than in the system architecture and design.

2.2 Threat Description

Identify and describe the system specific threats, environmentally based threats, and the impact these threats have on mission need. Definition of the potential threats must consider the intentional and unintentional events that can affect the integrity, confidentiality, and availability of the system.

2.3 Variances, Waivers, and Exceptions

Description of approved variances, waivers, and exceptions.

2.4 Network Connection Rules

If the system is to be connected to any other network or system, there may be additional requirements incurred by connection to that system. These requirements and those of other systems that may be connected to this system or network must be added to this section.

3. SYSTEM ARCHITECTURE DESCRIPTION

3.1 System Description

The architecture description provides the framework for the information system architecture and includes a description of the hardware, software, and interfaces. Against this framework, the architecture description stipulates the security architecture. Existing or planned system features that facilitate expansion or external connection should be mentioned in this section.

(5) Hardware. Identify and describe the hardware used and whether it is a standard commercial product or unique. Describe the target hardware and its function. Hardware is the physical equipment as opposed to programs, procedures, rules, and associated documentation.

Describe the significant features of the communications layout. Include a high level diagram of the communications links and encryption techniques connecting the components of the information system, associated data communications, and networks.

(6) Software. Identify and describe security relevant software. This includes manufacturer-supplied software, other commercial off-the-shelf software, and all program supplied security relevant applications software.

3.2 System Interfaces and External Connections

Describe the system's external interfaces. Descriptions of all interactions and connections with external systems must be included.

3.3 Accreditation Boundary

Describe the boundary of the system under consideration. The description must include diagrams or texts to clearly delineate which components are to be evaluated as part of the C&A task. All components included must be described in the systems description.

4. SYSTEM SECURITY REQUIREMENTS

4.1 Cyber Security Requirements

The system cyber security requirements are derived from the applicable NNSA approved PP(s) for all information groups on the information system. Include any additional requirements due to connection with other networks and systems.

These requirements will be documented in one or more STs based on NNSA approved PPs.

4.2 Data Security Requirements (expanded/increased requirements by data owner/ stewards)

In addition to the requirements defined in NNSA approved PP(s), there may be security requirements stipulated by data steward(s) and the DAA. The type of data to be processed may result in additional restrictions as determined by the data steward(s) or organizations that have access to the system or share data with the system.

5. Training

This section describes the training requirements, types of training, who is responsible for preparing and conducting the training,

3. Appendices. Each appendix of the sample SSP is briefly described below. The title for each appendix matches the sample SSP outline.

APPENDIX A. Definitions

APPENDIX B. Security Target(s)

PP/Security Requirements expressed as one or more Security Targets.

APPENDIX C. Security Test and Evaluation Plan and Procedures.

Contains all formal test and analysis results.

APPENDIX D. Certification Statement

CSSM recommendation regarding the accreditation of the information system.

APPENDIX E. Risk Assessment Results

This appendix includes an analysis of system assets and vulnerabilities to establish the risks in operating the system.

APPENDIX F. Approved Variances, Waivers, and Exceptions

APPENDIX G. CSOM Accreditation Recommendation

CSOM recommendation regarding the accreditation of the information system.

APPENDIX H. Contingency Plan(s)

This appendix should reference contingency or continuity of operation plans that describe the emergency responses, backup procedures, backup operations, and recovery of data. The information system environment, the criticality of the functional applications being supported and the user's requirements influences the detail of the plans.

APPENDIX I. Memorandums of Agreement – System Interconnect Agreements

APPENDIX J. Accreditation Documentation and Statement

This appendix contains the authorization to operate in a formal memorandum from the DAA to the element developing or operating the information system.